(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年6 月24 日 (24.06.2004)

PCT

(10) 国際公開番号
WO 2004/053666 A1

(51) 国際特許分類[7]: G06F 1/00

(21) 国際出願番号: PCT/JP2003/015779

(22) 国際出願日: 2003 年12 月10 日 (10.12.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-359597
2002 年12 月11 日 (11.12.2002) JP

(71) 出願人 (米国を除く全ての指定国について): インターレックス株式会社 (INTERLEX INC.) [JP/JP]; 〒108-0023 東京都 港区 芝浦２丁目１７番１３号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 佐藤 健次 (SATO,Kenji) [JP/JP]; 〒141-0021 東京都 品川区 上大崎３丁目１０番５９号パレロワイヤル目黒１０１号 Tokyo (JP).

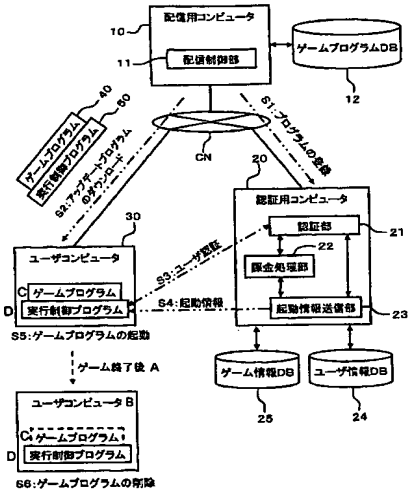
(74) 代理人: 上村 輝之, 外(KAMIMURA,Teruyuki et al.); 〒101-0035 東京都 千代田区 神田紺屋町１６ クニイビル２Ｆ Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: SOFTWARE EXECUTION CONTROL SYSTEM AND SOFTWARE EXECUTION CONTROL PROGRAM

(54) 発明の名称: ソフトウェア実行制御システム及びソフトウェアの実行制御プログラム



10...DISTRIBUTION COMPUTER
11...DISTRIBUTION CONTROL SECTION
12...GAME PROGRAM DB
40...GAME PROGRAM
50...EXECUTION CONTROL PROGRAM
S2...DOWNLOAD UPDATE PROGRAM
S1...REGISTER PROGRAM
30...USER COMPUTER
S3...USER AUTHENTICATION
S4...START INFORMATION
S5...GAME PROGRAM START
20...AUTHENTICATION COMPUTER
21...AUTHENTICATION SECTION
22...ACCOUNTING SECTION
23...START INFORMATION TRANSMISSION SECTION
A...AFTER GAME END
B...USER COMPUTER
C...GAME PROGRAM
D...EXECUTION CONTROL PROGRAM
S6...GAME PROGRAM DELETION
25...GAME INFORMATION DB
24...USER INFORMATION DB

(57) Abstract: It is possible to prevent unauthorized use of software such as a game program in download type software distribution for using a program and data by storing them in a user computer in advance. A user downloads (S2) a game program (40) of new version (including an accompanying data group) and an execution program (50) from a distribution computer (10). The execution control program (50) performs authentication by online with an authentication computer (20) and acquires (S3, S4) start information required for starting the game program (40). The execution control program (50) decodes the game program (40) according to the start information and starts it (S5). When the user terminates the game by terminating the game program (40), the execution control program (50) deletes all or a part of the game program (40) so as to incapacitate it (S6).

(57) 要約: 【課題】ユーザコンピュータに予めプログラムやデータを格納させて利用するダウンロード式のソフトウェア配信において、ゲームプログラム等のソフトウェアの違法な使用を未然に阻止する。【解決部】ユーザは、配信用コンピュータ10から新版のゲームプログラム40(付随データ群も含む)及び実行制御プログラム50をダウンロードする(S2)。実行制御プログラム50は、認証用コンピュータ20とオンラインによる認証を行って、ゲームプログラム40を起動させるために必要な起動情報を取得する(S3,S4)。実行制御プログラム50は、起動情報に基づいてゲームプログラム40をデコードし、起動させる(S5)。ユーザがゲームを終えて、ゲームプログラム40を終了させると、実行制御プログラム50は、ゲームプログラム40の全部又は一部を削除することにより無力化する(S6)。

WO 2004/053666 A1

(84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

ソフトウェア実行制御システム及びソフトウェアの実行制御プログラム

技 術 分 野

本発明は、例えば、ゲームソフトウェア、文書や図形等を作成する実務用ソフトウェア等の各種アプリケーションソフトウェアを新バージョンのソフトウェアに更新させたり、その実行を制御するソフトウェア実行制御システム及びソフトウェアの実行制御プログラムに関する。

技 術 背 景

一般的に、例えば、パーソナルコンピュータや携帯情報端末等のユーザコンピュータ上で稼働するゲームソフトウェア等のアプリケーションソフトウェアは、例えば、ＯＳ（Operating System）、使用言語、ハードウェア構成等の各種のソフトウェア実行環境に応じて、あるいは、ソフトウェアの価格や代金支払いの有無等に応じて、複数種類のバージョンが用意されることがある。

例えば、同じソフトウェアであっても、英語版、日本語版、中国語版等のように、使用言語毎に異なるバージョンが用意されることがある。また、無償で提供するバージョンと有償で提供するバージョンとを用意し、無償のソフトウェアから有償のソフトウェアへバージョンアップを誘導することも比較的よく行われている。無償のソフトウェアは、「体験版」や「お試し版」とも呼ばれ、有償のソフトウェアは「製品版」や「完全版」とも呼ばれる。無償のソフトウェアは、同種の有償のソフトウェアに比べて、その機能が一部制限されていたり、試用期間や試用回数に制限を受けることが多い。無償のソフトウェアを試用することにより

ソフトウェアの価値を認めたユーザは、提供元のウェブサイトから有償のソフトウェアを購入してダウンロードしたり、販売店で有償のパッケージソフトウェアを購入したりしてバージョンアップを行う。

一方、ソフトウェアはディジタルデータであり、複製が容易で、かつ複製による劣化も殆ど生じないという特徴を有するため、違法コピーや無断使用が大きな問題となっている。そこで、ソフトウェア（ソフトウェアのライセンス）を購入した正規ユーザとライセンスを得ていない違法ユーザとを、ユーザ認証等によって識別し、正規ユーザにのみソフトウェアを使用させるようにすることが従来より行われている。

例えば、ソフトウェアをインストールする際に、ソフトウェアパッケージや記録媒体に印刷されたプロダクトＩＤを入力させて、正規購入品であるか否かを判定する技術は知られている（例えば、特開２００２－２５８９６３号公報　段落０００３参照）。

また、ソフトウェアを使用するための鍵データを、イントラネット上に設置されたライセンス管理サーバに要求し、ユーザ認証により正当なユーザと認められた場合には、ライセンス管理サーバから鍵データを取得し、この鍵データによってソフトウェアを起動させて使用するようにしたものも知られている（例えば、特開２００２－６９７２号公報、特開２００２－２９７２５４公報）。

プロダクトＩＤ（プロダクトキー）を入力することにより正規ユーザであるか否かを判別する従来技術は、単なる文字や記号からなるＩＤをインストール時に入力するだけの防御機構であり、容易に回避可能である。従って、この種の防御機構（著作権保護機構）しか備えないソフトウェアは、違法コピーや無断使用を事実上排除することができない。

ライセンス管理サーバとの間でユーザ認証を行い、正常に認証された場合に鍵データをユーザコンピュータに送信して起動させる技術は、単にプロダクトＩＤ

を入力するだけの技術に比べて、防御力は向上している。しかし、ソフトウェアはユーザコンピュータ上で既に起動可能状態に置かれており、鍵データの取得待ちとなっている。従って、鍵データの入力待ち状態となっているソフトウェアを違法コピーし、別の方法で鍵データを取得してしまえば、防御機構をすり抜けて使用することができる。

一方、近年では、コンピュータの処理能力増大及び通信ネットワークの高速化等に伴って、ユーザが希望する時に希望のソフトウェアを実行させる方法が提案されている。このようなソフトウェアのオンデマンド配信に適用可能な配信方法としては、ストリーミング方式とダウンロード方式とが知られている。

ストリーミング方式では、ユーザコンピュータは、サーバからソフトウェアを受信しながら同時に再生を行う。そして、再生を終了して不要になったデータは直ちに破棄される。従って、ストリーミング方式は、ユーザの閲覧が終了した時点でデータが残らないため、特殊なソフトウェアを用いる等しない限り、違法にソフトウェアをコピーすることができない。しかし、ストリーミング方式では、ユーザが視聴を希望するたび毎に毎回ソフトウェアのデータを送信する必要があるため、広帯域で高速な通信ネットワークが整備されている場合でも、多数のユーザが同時にストリーミング配信を希望すると、通信ネットワークのトラフィックが増大し、サーバの負担も大きくなる。

これに対し、ダウンロード方式の場合は、ユーザの希望するソフトウェアをサーバからユーザコンピュータにダウンロードさせて蓄積し、ユーザコンピュータ上で実行させるため、データが通信ネットワークを流れる時間は少なく、多数のユーザからの配信要求に応えることができる。しかし、ダウンロード方式の場合は、ユーザコンピュータ内にソフトウェアが蓄積されたままになるため、ストリーミング方式よりも簡単に違法コピー等を行うことができる。

また、例えば、CD－ROM、DVD－ROM、ハードディスク、半導体メモリ等

の各種記録媒体にゲームプログラム等を固定して流通に置くことも広く行われている。この場合も、上述の通り、ゲームプログラム等が不正にコピーされたり、プロテクト機構が不正に破られたりして、不正に使用されている。

発明の開示

そこで、本発明の１つの目的は、ソフトウェアの不正使用を抑制できるようにしたソフトウェア実行制御システム及びソフトウェアの実行制御プログラムを提供することにある。

本発明の１つの目的は、ユーザコンピュータにソフトウェアを保存して実行させるダウンロード方式の場合に、違法コピーや無断使用を防止できるようにしたソフトウェア実行制御システム及びソフトウェアの実行制御プログラムを提供することにある。

本発明の１つの目的は、ソフトウェアの実行中に不正な使用が行われるのを未然に防止できるようにしたソフトウェア実行制御システム及びソフトウェアの実行制御プログラムを提供することにある。

本発明の１つの目的は、負荷状態等を考慮しながら、不正使用に対する監視効率を動的に制御することができるソフトウェア実行制御システム及びソフトウェアの実行制御プログラムを提供することにある。

本発明の他の目的は、後述する実施の形態の説明から明らかになるであろう。

本発明に係るソフトウェア実行制御システムは、ユーザコンピュータにインストールされた第１のソフトウェアを第２のソフトウェアに更新させるものであって、後述の配信部及び認証部を備え、かつ、特徴的な動作を行う実行制御プログラムを採用する。

配信部は、エンコードされた第２のソフトウェア及び該第２のソフトウェアの

実行を制御するための実行制御プログラムをユーザコンピュータに通信ネットワークを介して配信するものである。認証部は、ユーザコンピュータにインストールされた実行制御プログラムからの要求によってユーザ認証を行い、正当なユーザであると確認した場合には、第２のソフトウェアをデコードして起動させるために必要な所定の情報を通信ネットワークを介して実行制御プログラムに送信するものである。そして、第２のソフトウェアは実行制御プログラムから渡される起動情報のみで起動可能に構成されており、実行制御プログラムは、（１）認証部から受信した所定の情報に基づいてエンコードされた第２のソフトウェアをデコードして第１のソフトウェアに置き換え、（２）所定の情報に基づいて起動情報を生成することにより、第２のソフトウェアを起動させ、（３）第２のソフトウェアの実行が終了された場合には、第２のソフトウェアを無力化させるように構成されている。

第１のソフトウェアと第２のソフトウェアとは、同一種類のソフトウェアであって、バージョンの異なるものである。第１のソフトウェアを旧版ソフトウェア、第２のソフトウェアを新版ソフトウェアと呼ぶこともできる。第１，第２のソフトウェアとしては、例えば、ゲーム、映画、娯楽番組、教養番組、教育番組、文書作成、図形作成、画像編集等の各種アプリケーションソフトウェアを採用することができる。第１のソフトウェアと第２のソフトウェアとは、例えば、使用言語、実行可能環境（対応ＯＳ等）、機能制限の有無等で相違する。ユーザコンピュータとしては、例えば、ワークステーション、パーソナルコンピュータ、携帯情報端末、携帯電話等を挙げることができる。

最初に、ユーザコンピュータにインストールされている第１のソフトウェアは、後述の認証処理等を行わずに、ユーザが自由に使用することができる。第１のソフトウェアは、例えば、ソフトウェアベンダーのサイトからインターネット等の通信ネットワークを介して、あるいは、店頭販売のパッケージソフトウェアによ

って、ユーザコンピュータにインストールされている。

次に、ユーザが、配信部から第２のソフトウェアのダウンロードを希望すると、第２のソフトウェア及び第２のソフトウェアの実行を制御する実行制御プログラムが配信部からユーザコンピュータに送信される。実行制御プログラムは、ユーザコンピュータ上で実行される。実行制御プログラムは、通信ネットワークを介して認証部にユーザ認証を要求する。ユーザ認証の方法としては、例えば、ユーザＩＤ、パスワード、ユーザコンピュータに固有の情報（例えば、MAC アドレス（Media Access Control address）等）を予め登録されているデータと照合することにより行うことができる。なお、これに限らず、例えば、指紋や声紋等のユーザ固有の生体情報を用いて認証を行うようにしてもよい。

認証部が正当なユーザであると認証した場合は、認証部からユーザコンピュータの実行制御プログラムに向けて、所定の情報が送信される。この所定の情報には、エンコードされた状態でユーザコンピュータに送信された第２のソフトウェアをデコードし、デコードされた第２のソフトウェアを起動させるために必要なデータが含まれている。

ここで、第２のソフトウェアは、実行制御プログラムから渡される起動情報のみで起動可能に構成されている。即ち、実行制御プログラムは、第２のソフトウェアを起動させる専用の「ランチャーソフトウェア」として作用する。

そして、実行制御プログラムは、以下の処理を行う。（１）まず、実行制御プログラムは、認証部から受信した所定の情報に基づいて（所定の情報に含まれるデコードキーを利用して）、第２のソフトウェアをデコードする。デコードされた第２のソフトウェアは、第１のソフトウェアに置き換えられる。（２）次に、実行制御プログラムは、認証部から受信した所定の情報に基づいて（所定の情報に含まれる起動引数を利用して）、起動情報（起動引数とデコードされた第２のソフトウェアのレジストリパスからなる起動ステートメント）を生成し、この起動情報に

よって第２のソフトウェアを起動させる。これにより、ユーザは、ユーザコンピュータ上で第２のソフトウェアを使用することができる。（３）実行制御プログラムは、第２のソフトウェアの起動後も、第２のソフトウェアの実行状態を監視しており、第２のソフトウェアの実行終了を検出すると、第２のソフトウェアを無力化させる。これにより、ユーザは、第２のソフトウェアを使用することができなくなる。

ユーザが再度の使用を希望する場合、再び認証部による認証を受けて所定の情報を取得すればよい。あるいは、再びユーザコンピュータを配信部にアクセスさせて、第２のソフトウェアを再度ダウンロードしてもよい。第２のソフトウェアの全体を再度ダウンロードする必要はなく、プログラム部分のみを再ダウンロードするように構成すれば、通信時間を短縮し、トラフィックを低減させることができる。なお、認証部からユーザコンピュータに向けて送信される所定の情報は、暗号化されているのが好ましい。

第２のソフトウェアの実行が終了すると、実行制御プログラムは、第２のソフトウェアを無力化させる。無力化とは、第２のソフトウェアを起動したり、実行したりできなくすることを意味する。無力化の方法としては、種々のものを採用することができる。例えば、デコードされた第２のソフトウェアの全体を削除することにより無力化することができる。また、デコードされた第２のソフトウェアの一部を削除することによっても無力化することができる。なお、一部のみを削除する場合は、その削除した部分及び起動引数を認証部から受信することにより、第２のソフトウェアを再起動させることができる。あるいは、第２のソフトウェアがプログラムと付随データ群とを含んでなる場合、プログラムのみを削除することでも第２のソフトウェアを無力化させることができる。なお、デコード前のエンコードデータを保存しておくことにより、認証部から所定の情報を再度受信するだけで第２のソフトウェアを再び使用することができる。付随データ群

とは、プログラムの実行に際して利用されるプログラム以外のデータ群を意味し、例えば、画像データ、音声データ、楽曲データ、テキストデータ等を挙げることができる。

好適な実施形態では、実行制御プログラムは、複数種類の第２のソフトウェアに対応可能に構成されており、認証部が実行制御プログラムに送信する所定の情報には、起動させる第２のソフトウェアの格納先アドレス情報と起動引数と第２のソフトウェアをデコードするためのデコードキー情報とが含まれる。

通信ネットワークを介したリアルタイムのオンライン認証と第２のソフトウェアの起動及び終了を制御する実行制御プログラムは、第２のソフトウェアとは別体に生成されている。従って、１種類の実行制御プログラムを用意するだけで、多種類の第２のソフトウェアに対応することができる。

好適な実施形態では、実行制御プログラムは、ユーザコンピュータに固有のマシン情報と暗号化キー情報とを含む認証用情報を認証部に送信し、認証部は、少なくともマシン情報に基づいてユーザ認証を行い、正当なユーザであると確認した場合には、所定の情報を暗号化キー情報で暗号化して通信ネットワークを介して実行制御プログラムに送信するものであり、かつ、認証部には、マシン情報を複数個登録可能に構成されている。

ユーザコンピュータに固有のマシン情報としては、例えば、MAC アドレス等を挙げることができる。これに加えて、ユーザコンピュータの構成情報（例えば、搭載メモリ量、ＣＰＵスペック、サウンドチップやグラフィックアクセラレータの製品名等）を採用してもよい。認証部には、複数個のマシン情報を登録させることができる。これにより、第２のソフトウェアのライセンスを正当に購入したユーザは、例えば、自宅のパーソナルコンピュータと職場のパーソナルコンピュータ等のように、複数台のユーザコンピュータを用いて、同一の第２のソフトウェアを利用することができる。

好適な実施形態では、認証部は、正当なユーザであると確認した場合には、該ユーザが起動可能な第２のソフトウェアの一覧データをユーザコンピュータに送信し、一覧データから選択された第２のソフトウェアに関する所定の情報を通信ネットワークを介して実行制御プログラムに送信する。

ユーザが複数種類の第２のソフトウェアのライセンスを正式に購入済の場合もあるが、認証部は、ユーザ認証後に、そのユーザが利用可能な第２のソフトウェアの名称等を列挙した一覧データをユーザコンピュータに送信する。ユーザは、起動可能な（利用可能な）一覧メニューから起動を望む第２のソフトウェアを選択する。これにより、認証部は、選択された第２のソフトウェアをデコードし起動するための所定の情報を生成し、実行制御プログラムに送信する。

好適な実施形態では、実行制御プログラムは、ユーザコンピュータに固有のマシン情報を取得する機能と、暗号化キー情報を生成する機能と、認証部にユーザ認証を要求し、少なくともマシン情報及び暗号化キー情報を認証部に送信する機能と、認証部から受信した起動可能な第２のソフトウェアの一覧データからいずれか１つの第２のソフトウェアをユーザに選択させ、選択された第２のソフトウェアを認証部に通知する機能と、選択された第２のソフトウェアのユーザコンピュータにおける格納先アドレス情報と起動引数とデコードキー情報とを少なくとも暗号化キー情報により暗号化してなる所定の情報を受信する機能と、暗号化された所定の情報を少なくとも暗号化キー情報により解読する機能と、解読されたデコードキー情報によりユーザコンピュータ内の第２のソフトウェアをデコードさせる機能と、解読された起動引数及び格納先アドレス情報に基づいて、起動情報を生成する機能と、生成された起動情報によってデコードされた第２のソフトウェアを起動させる機能と、起動された第２のソフトウェアの実行状態を監視し、該第２のソフトウェアの実行が終了した場合は、第２のソフトウェアを無力化させる機能と、をユーザコンピュータ上に実現させる。

また、好適な実施形態では、第２のソフトウェアは、プログラムと付随データ群とを含んでなり、プログラム又は付随データ群の少なくともいずれか一方を更新させるようになっている。

ここで、ユーザコンピュータにインストールされている第１のソフトウェアは、第２のソフトウェアに置換されるまでは、認証部による認証を受けることなく実行可能である。

また、好適な実施形態では、実行制御プログラムは、第２のソフトウェアとは別に強制終了させることができないプログラムとして構成されている。

即ち、例えば、稼働中のタスクを管理するプログラム等を用いて、実行制御プログラムのみを強制終了させることができないように構成されている。実行制御プログラムによる監視を停止させて、第２のソフトウェアのみをコピー等できないようにするためである。より具体的には、ハードウェアを指定しないデバイスドライバとして実行制御プログラムを生成すれば（ハードウェアを指定しないので、厳密にはデバイスドライバではないが）、アプリケーションプログラムよりもＯＳ側に近いプログラムあるいはＯＳの一部を構成するプログラムとして構成されるため、通常のアプリケーションプログラムのように強制的に終了させることが困難となる。強制終了させにくいプログラムとしては、ドライバプログラムの他にＢＩＯＳ（Basic Input/Output System）も知られている。しかし、BIOS は、基本的に、ハードウェアとの間で直接データを送受信するだけの機能しか持たないため、暗号化されたデータを復号化したり、第２のソフトウェアの実行を監視したりする等の高度な制御を行うことができない。このように、実行制御プログラムを、例えば、デバイスドライバのように、ＯＳとアプリケーションプログラム（第２のソフトウェア）との間に位置する中間プログラムとして構成することにより、高度な処理を行わせつつ、悪用を防止することができる。

好適な実施形態では、配信部と認証部とは、それぞれ別体のコンピュータ上に

実現されている。

例えば、第２のソフトウェア及び実行制御プログラムを配信する配信部は、各ソフトウェア会社毎にそれぞれ設置し、第２のソフトウェアの起動時認証を行う認証部は、各国、各地域、各ソフトウェア会社の団体毎に設置することができる。

本発明は、プログラムの発明としても把握することができる。

即ち、ユーザコンピュータにインストールされた第１のソフトウェアを第２のソフトウェアに更新し、この第２のソフトウェアの実行を制御する実行制御プログラムであって、外部の認証部と通信ネットワークを介して通信し、ユーザ認証を求める第１の機能と、認証部から受信した所定の情報に基づいて、第２のソフトウェアを起動させるための起動情報を生成する第２の機能と、認証部から受信した所定の情報に基づいて、第２のソフトウェアをデコードさせる第３の機能と、ユーザコンピュータに既にインストールされている更新前のソフトウェアをデコードされた第２のソフトウェアに置き換える第４の機能と、生成された起動情報によって第２のソフトウェアを起動させる第５の機能と、第２のソフトウェアの実行状態を監視し、第２のソフトウェアの実行が終了した場合は、第２のソフトウェアを無力化させる第６の機能と、をユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

また、本発明は、ソフトウェアの更新方法としても把握できる。

即ち、ユーザコンピュータにインストールされている自由に使用可能な第１のソフトウェアを第２のソフトウェアに更新可能である旨をユーザに通知させるステップと、第２のソフトウェアを配信する配信用コンピュータにユーザコンピュータを通信ネットワークを介して接続させ、第２のソフトウェアへの更新を要求させるステップと、配信用コンピュータからユーザコンピュータにエンコードされた第２のソフトウェア及び該第２のソフトウェアの実行を制御するための実行制御プログラムを通信ネットワークを介して送信させるステップと、ユーザコン

ピュータ上で起動した実行制御プログラムにより、ユーザコンピュータと認証用コンピュータとを通信ネットワークを介して接続させ、認証用コンピュータにユーザ認証を要求させるステップと、ユーザ認証により正当なユーザであると認められた場合に認証用コンピュータからユーザコンピュータに送信される所定の情報に基づいて、第２のソフトウェアをデコードするステップと、認証用コンピュータから受信した所定の情報に基づいて、第２のソフトウェアを起動させるための起動情報を生成させるステップと、生成された起動情報によって第２のソフトウェアを起動させるステップと、起動された第２のソフトウェアの実行を監視し、第２のソフトウェアの実行が終了した場合は、第２のソフトウェアを無力化させるステップと、を含んでなるソフトウェアの更新方法。

本発明の他の観点に従う管理用コンピュータは、アプリケーションソフトウェア及び監視プログラムと共にユーザコンピュータにインストールされる実行制御プログラムと通信を行うことにより、実行制御プログラムの動作を制御するものである。そして、この管理用コンピュータは、実行制御プログラムからの要求に基づいてユーザ認証を行う認証部と、認証部により正当なユーザであると確認された場合は、実行制御プログラムがアプリケーションソフトウェアを起動させるために必要な第１の情報を実行制御プログラムに送信する情報送信部と、所定の時期に実行制御プログラムとの間で行われる継続確認通信に基づいて、アプリケーションソフトウェアの実行継続を許可するか否かを管理する継続実行管理部と、を備えている。

本発明の一態様では、継続実行管理部は、継続確認通信によって実行制御プログラムから取得される第１の識別情報とユーザ認証に予め関連付けられている第２の識別情報とを比較し、両方の識別情報が対応する場合は、実行制御プログラムに対してアプリケーションソフトウェアの実行継続を許可し、各識別情報が対応していない場合は、実行制御プログラムに対してアプリケーションソフトウェ

アの実行継続を禁止させる。

本発明の一態様では、継続実行管理部は、第２の識別情報に対応する第１の識別情報を予め実行制御プログラムに設定させる。

本発明の一態様では、継続実行管理部は、所定の時期を実行制御プログラムに予め設定し、この予め設定された所定の時期が到来した場合は、実行制御プログラムから継続実行管理部に対して継続確認通信を行わせる。

本発明の一態様では、継続実行管理部は、所定の時期を可変に設定可能となっている。

本発明の一態様では、継続実行管理部は、少なくとも予測される将来の負荷状態を考慮して、所定の時期を可変に設定可能である。

本発明の一態様では、監視プログラムは、アプリケーションソフトウェア及び実行制御プログラムの動作状態をそれぞれ監視し、アプリケーションソフトウェアまたは実行制御プログラムのいずれか一方が動作を停止した場合は、アプリケーションソフトウェア及び実行制御プログラムをそれぞれ停止させ、自身も停止させるものであり、実行制御プログラムは、アプリケーションソフトウェア及び監視プログラムの動作状態をそれぞれ監視し、アプリケーションソフトウェアまたは監視プログラムのいずれか一方が動作を停止した場合は、アプリケーションソフトウェア及び監視プログラムをそれぞれ停止させ、自身も停止させるものである。

本発明のさらに別の観点に従うコンピュータプログラムは、コンピュータを、アプリケーションソフトウェアの実行を制御する実行制御部と、アプリケーションソフトウェア及び実行制御部の動作状態をそれぞれ監視する監視部として、機能させるものであって、実行制御部は、管理用コンピュータと通信することによりユーザ認証を要求する機能と、管理用コンピュータから受信した第１の情報に基づいて、アプリケーションソフトウェアを起動させる機能と、管理用コンピュ

ータとの間で継続確認通信を行う機能と、継続確認通信によってアプリケーションソフトウェアの実行継続が禁止された場合は、アプリケーションソフトウェアの動作を停止させる機能と、を備え、監視部は、アプリケーションソフトウェア及び実行制御部の動作状態をそれぞれ監視する機能と、アプリケーションソフトウェアまたは実行制御部のいずれか一方が動作を停止した場合は、アプリケーションソフトウェア及び実行制御部をそれぞれ停止させ、自身も停止させる機能と、を備えている。

図面の簡単な説明

図１は、本発明の実施形態に係るソフトウェア実行制御システムの全体概要を示す説明図である。

図２は、データベース等の構造を示し、（ａ）はユーザ情報データベースを、（ｂ）はゲーム情報データベースを、（ｃ）はＨＴＭＬヘッダ内に暗号化された起動情報を埋め込んで送信する様子を、それぞれ示す。

図３は、プログラムの概略構造を示し、（ａ）はゲームプログラムを、（ｂ）は実行制御プログラムの構造を、それぞれ示す。

図４は、ユーザコンピュータにインストールされた旧版のゲームプログラムを、新版のゲームプログラムに更新し、起動を制御する様子を示す説明図である。

図５は、ゲームプログラム及び実行制御プログラムをインストールするときの処理を示すフローチャートである。

図６は、実行制御プログラム及び認証用コンピュータとの間で行われるオンライン認証等を示すフローチャートである。

図７は、

本発明の他の実施形態に係るソフトウェア実行制御システムの全体概要を示す説明図である。

図８は、データベース等の構造を示し、（ａ）はユーザ情報データベースを、（ｂ）はゲーム情報データベースを、（ｃ）は監視状況データベースを、それぞれ示す。

図９は、ソフトウェア実行制御システムの全体動作の概要を示すフローチャートである。

図１０は、周期的に行われる継続確認通信の処理概要を示すフローチャートである。

図１１は、次回の継続確認通信を行う時期を決定する処理の概要を示すフローチャートである。

図１２は、ゲームマネージャ及び監視プログラムがそれぞれ相互に監視する処理の概要を示すフローチャートである。

図１３は、本発明のさらに別の実施形態に係るソフトウェア実行制御システムの全体概要を示す説明図である。

発明を実施するための最良の形態

以下、本発明の実施形態を図１～図１３を参照しつつ詳細に説明する。

まず、図１～図６に基づいて第１実施例を説明する。図１は、ソフトウェア実行制御システムの全体概要を示す説明図である。本実施例では、ゲームプログラムをオンラインで更新させるシステムを例に挙げて説明する。

配信用コンピュータ１０は、新版のゲームプログラム４０及び実行制御プログラム５０を、インターネット等の通信ネットワークを介して、各ユーザのコンピュータ３０に配信するためのものである。配信用コンピュータ１０は、各ソフト

ウェア会社（ベンダー）毎にそれぞれ設置されるサーバとして構成することができる。

まず、配信用コンピュータ１０は、ゲームプログラムデータベース１２に登録された新版プログラムについて、事前に、認証用コンピュータ２０に登録を行う（Ｓ１）。例えば、新版ゲームプログラムの名称、種類、販売価格、データサイズ、バージョン情報等のデータが、配信用コンピュータ１０から認証用コンピュータ２０に登録される。もっとも、配信用コンピュータ１０と認証用コンピュータとが一体的に構成されている場合は、このような外部ネットワークを介した通知は必ずしも必要ない。

配信用コンピュータ１０の配信制御部１１は、ユーザコンピュータ３０からプログラムの更新要求を受けると、ユーザの希望するゲームプログラム４０をゲームプログラムデータベース１２から読み出して、ユーザコンピュータ３０に配信するようになっている（Ｓ２）。ここで、新版のゲームプログラム４０は、単独でユーザコンピュータ３０に配信されるのではなく、ゲームプログラム４０の起動や削除等を管理する実行制御プログラム５０と共にユーザコンピュータ３０に配信される点に留意すべきである。

認証用コンピュータ２０は、例えば、複数のソフトウェア会社が所属する団体や機関毎にそれぞれ設置されるサーバとして構成することができる。また、これに限らず、各ソフトウェア会社毎に認証用コンピュータ２０をそれぞれ設置してもよい。認証用コンピュータ２０は、認証部２１と、課金処理部２２と、起動情報送信部２３と、ユーザ情報データベース２４と、ゲーム情報データベース２５とを備えている。

認証部２１は、ユーザコンピュータ３０の実行制御プログラム５０から送信される所定の認証用データに基づいて、ユーザ認証を行うものである。詳細は後述するが、認証用データには、例えば、ユーザ識別情報（ユーザＩＤ）、パスワード

（ＰＷ）、MACアドレス（Media Access Control address）が含まれる。

課金処理部２２は、新版ゲームプログラム４０の使用許諾に際して、ユーザに課金するものである。課金方法には、種々のものを採用できる。例えば、ゲームプログラムの代金を一括でユーザに支払わせたり（売り切り）、又は、ユーザがゲームプログラムを使用する毎に課金してもよい。あるいは、所定期間や所定回数毎に課金するようにしてもよい。なお、支払方法も、例えば、クレジット決済、電子マネー決済等のように種々のものを採用できる。

起動情報送信部２３は、ユーザコンピュータ３０の記憶装置（例えば、ハードディスク等）に格納された新版のゲームプログラム４０をデコードし、起動させるために必要な起動情報をユーザコンピュータ３０の実行制御プログラム５０に向けて送信するものである。

ユーザが、実行制御プログラム５０を介して認証用コンピュータ２０の認証部２１と認証を行い、ゲームプログラム４０の購入代金（使用権の代金）を支払い済みの正当なユーザであると認証された場合は（Ｓ３）、起動情報送信部２３から起動情報が実行制御プログラム５０に送信される（Ｓ４）。ゲームプログラム４０の代金を未払いのユーザが認証用コンピュータ２０にアクセスした場合は、課金処理部２２を介して課金処理が行われた後、起動情報が実行制御プログラム５０に向けて送信される。

さて、ユーザコンピュータ３０の構成に目を転じると、ユーザコンピュータ３０は、例えば、パーソナルコンピュータ、ワークステーション、携帯情報端末、携帯電話等のコンピュータとして構成されている。ユーザコンピュータ３０は、演算処理装置（ＣＰＵ）、主記憶、補助記憶、外部入出力回路等のコンピュータ資源を必要に応じて備えており、これらの各資源は適宜ゲームプログラム４０及び実行制御プログラム５０によって使用される。

配信用コンピュータ１０からユーザコンピュータ３０に送信された新版のゲー

ムプログラム４０及び実行制御プログラム５０は、後述のように、付属するインストーラによってユーザコンピュータ３０にインストールされる。そして、実行制御プログラム５０が認証用コンピュータ２０との間でユーザ認証を行い、起動情報を入手すると、ゲームプログラム４０が起動される（Ｓ５）。なお、新版のゲームプログラム４０をインストールするより前に、ユーザコンピュータ３０に既にインストールされていた旧版のゲームプログラムは、新版のプログラムに置き換えられるため、以後使用することができなくなる。

ユーザは、ユーザコンピュータ３０を介して新版のゲームプログラム４０を利用することができる。そして、ユーザがゲームを終えて、ゲームプログラム４０を終了させると、実行制御プログラム５０は、ゲームプログラム４０を削除する等して無力化する（Ｓ６）。ユーザがゲームプログラム４０を再び利用する場合は、認証用コンピュータ２０に再度アクセスしてユーザ認証を行い、起動情報を取得する。

ここで、ユーザコンピュータ３０の記憶装置内には、新版のゲームプログラム４０がデコード前の暗号化ファイルの状態で保存されているため、ゲームプログラム４０を再使用する場合は、この暗号化ファイルをデコードするための情報（デコードキー）と起動させるための情報とを認証用コンピュータ２０から取得するだけでよい。即ち、本実施例では、ユーザコンピュータ３０のローカルディスクに新版ゲームプログラム４０を暗号化ファイルの状態で保存しておき、ゲームを行うたびに、認証用コンピュータ２０との間でオンライン認証を行って、暗号化されたゲームプログラム４０をデコードして起動させる。そして、ゲーム終了後には、デコードされたゲームプログラム４０を削除して無力化させる。

次に、図２は、認証用コンピュータ２０が利用するユーザ情報データベース２４及びゲーム情報データベース２５の構造例を示す説明図である。なお、図２に示す各データベース２４，２５の内容は一例であって、図示する項目の全てを備

える必要はない。

図２（ａ）に示すユーザ情報データベース２４は、例えば、ユーザＩＤと、パスワードと、複数の MAC アドレス１～ｎと、購入済のゲームプログラムを特定するゲームＩＤ１～ｎと、その他の情報とをそれぞれ対応付けることにより構成されている。ここで、複数の MAC アドレス１～ｎを登録可能としたのは、１人のユーザがそれぞれ異なる複数のユーザコンピュータ３０を用いて、ゲームプログラム４０を使用する場合も考慮したためである。従って、ユーザは、例えば、職場のコンピュータ、自宅のコンピュータ等の異なる情報処理端末を介して、ゲームプログラム４０を利用できるようになっている。その他の情報としては、例えば、ユーザの氏名、年齢、住所、ゲームのプレイ回数、獲得したポイント数（例えば、ゲーム購入代金やプレイ回数等に応じてポイントを与えるような場合）等を挙げることができる。

図２（ｂ）に示すゲーム情報データベース２５は、例えば、ゲームＩＤと、ゲーム名と、ゲーム情報（ゲームプログラムのレジストリパスを示す情報）と、暗号化されたゲームプログラム４０を復号するためのデコードキーと、デコードされたゲームプログラム４０を起動させるための起動引数と、その他の情報とをそれぞれ対応付けることにより構成されている。その他の情報としては、例えば、ゲームの種類（ロールプレイイングゲーム、格闘ゲーム、成人指定の有無等）、データサイズ、著作権管理情報等を挙げることができる。

図２（ｃ）に示すように、ゲーム情報、デコードキー及び起動引数は、暗号化されてＨＴＭＬ（Hyper Text Markup Language）データに埋め込まれ、ユーザコンピュータ３０に送信されるようになっている。即ち、ユーザコンピュータ３０側で生成された暗号化キー及び MAC アドレスによって、起動情報（ゲーム情報、デコードキー、起動引数）は暗号化され、例えば、ＨＴＭＬのヘッダ部に埋め込まれる。従って、認証用サーバ２０は、ユーザコンピュータ３０からの HTTP

(Hyper Text Transport Protocol) リクエストに応じて、暗号化された起動情報を生成し、この暗号化された起動情報を含んだ HTTP レスポンスをユーザコンピュータ３０に返すようになっている。

次に、図３は、ゲームプログラム４０及び実行制御プログラム５０の概略構成を示す説明図である。

図３（ａ）に示すように、ゲームプログラム４０は、プログラム本体４１と、付随データ群４２とを含んでいる。付随データ群４２としては、例えば、動画像データ、静止画像データ、グラフィックスデータ、楽曲データ、音声データ、テキストデータ等を挙げることができる。

新版のゲームプログラム４０は、旧版のプログラムに比較して、プログラム４１又は付随データ群４２のいずれか又は双方が新しく作成されている。プログラム本体４１及び付随データ群４２の両方が旧版よりも新しい場合は、プログラム本体４１及び付随データ群４２の両方が新版に置き換えられる。付随データ群４２のみが新しい場合及びプログラム本体４１のみが新しい場合は、付随データ群４２又はプログラム本体４１のいずれかが新版に置き換えられる。

図３（ｂ）に示すように、実行制御プログラム５０は、ユーザコンピュータ３０上で、暗号用情報生成部５１と、認証要求部５２と、ゲーム選択部５３と、暗号解読部５４と、起動部５５と、デコード部５６と、実行監視部５７という各機能を実現させる。一例として、実行制御プログラム５０は、デバイスを特定しないデバイスドライバとして構成されている。このため、実行制御プログラム５０は、例えば、ゲームプログラム等のアプリケーションプログラムとは異なって、タスク管理プログラム等から終了させることができないように構成することができる。

暗号情報生成部５１は、例えば、ユーザコンピュータ３０の内蔵タイマから取得した時刻情報に基づいて暗号化キーを生成するほか、ユーザコンピュータ３０

のMACアドレス等を取得する。

認証要求部５２は、ユーザコンピュータ３０に実装されているネットワークアクセスの機能を内部的に呼び出して、認証用コンピュータ２０にアクセスし、暗号化キー、MAC アドレス、ユーザＩＤ及びパスワードを認証用コンピュータ２０に送信してユーザ認証を求める。

ゲーム選択部５３は、ユーザ認証が終了して認証用コンピュータ２０からユーザコンピュータ３０に送信された一覧メニューから、ユーザが希望するゲームを選択させる。この一覧メニューは、ユーザが利用可能な（起動可能な）ゲームプログラムを一覧形式で表示させるものであり、ユーザ情報データベース２４の購入済ゲームＩＤに基づいて生成することができる。

暗号化情報生成部５１によって生成された暗号化キー及び MAC アドレスにより、ユーザの選択したゲームプログラム４０を起動させるための起動情報は、暗号化されてユーザコンピュータ３０に送信される。暗号解読部５４は、暗号化キー及びMACアドレスに基づいて、暗号化された起動情報を解読する。

デコード部５６は、解読されたデコードキーによって、暗号化されたゲームプログラム４０をデコードさせる。なお、暗号化ファイルはそのまま保存される。起動部５５は、解読されたゲーム情報及び起動引数に基づいて、起動ステートメントを生成し、デコードされたゲームプログラム４０を起動させる。起動ステートメントは、ゲームプログラムのレジストリパスと起動引数から構成される。

ゲームプログラム４０が起動されると、実行監視部５７は、ゲームプログラム４０の実行状態を監視し、ゲームプログラム４０が終了すると、デコードされたプログラム本体４１を削除する。なお、デコードした付随データ群も一緒に削除してもよい。また、削除する場合は、プログラム又はデータの全部を削除してもよいし、一部を削除してもよい。

次に、図４は、本システムによってゲームプログラムを最新版に更新する様子

を模式的に示す説明図である。

まず、図４（ａ）に示すように、ユーザコンピュータ３０には、旧版のゲームプログラムが既にインストールされている。なお、図中では、バージョンアップ前の旧版のゲームプログラムを「初期プログラム」と、バージョンアップする新版のゲームプログラムを「更新版プログラム」とそれぞれ表示する。

ユーザは、例えば、CD-ROM、DVD-ROM、メモリ等の記録媒体に固定された旧版のゲームプログラム４０Ａをユーザコンピュータ３０にインストールして利用する（Ｓ１１）。あるいは、インターネット等の通信ネットワークを介して旧版のゲームプログラム４０Ａを取得することもできる。この旧版のゲームプログラム４０Ａは、認証用コンピュータ２０とのオンライン認証を受けることなく使用可能である。但し、本更新システムによっていったん更新された後は、更新版プログラムが旧式になった場合でも、オンライン認証を受けなければ利用することはできない。

旧版のゲームプログラム４０Ａを利用するユーザには、新版ゲームプログラム４０へアップデート可能である旨が通知される。この通知は、種々の方法で行うことができる。

第１の方法は、例えば、旧版のゲームプログラム４０Ａが、積極的又は消極的に、ユーザに新版のゲームプログラム４０へ更新可能であることを通知し、併せて、配信用コンピュータ１０のＵＲＬ（Uniform Resource Locator）を表示する方法である。積極的な通知としては、例えば、ゲーム開始時や終了時等に更新可能である旨及び配信用コンピュータ１０のＵＲＬを画面に表示させることが考えられる。消極的な通知としては、例えば、旧版のゲームプログラム４０Ａのヘルプメニューの中に、更新可能である旨及び配信用コンピュータ１０のＵＲＬを表示させることが考えられる。いずれの場合も、ＵＲＬをクリックするだけで、ウェブブラウザ３１を起動させ、自動的にユーザコンピュータ３０を配信用コンピュ

ータ１０にアクセスさせるように構成すると、ユーザの使い勝手が良い。

第２の方法は、電子的な媒体を介して積極的又は消極的に、新版のゲームプログラム４０へ更新可能である旨及び配信用コンピュータ１０のＵＲＬを、ユーザに通知する方法である。積極的な通知としては、例えば、ユーザ宛の電子メールを挙げることができる。消極的な通知としては、例えば、ウェブ上のサイト（例えば、配信用コンピュータ１０等）で、新版のゲームプログラム４０を広告宣伝することが考えられる。

第３の方法としては、その他、ゲーム雑誌やコンピュータ雑誌等の紙媒体上での広告宣伝、ネットワーク上に形成されたゲームプログラム同好会のようなコミュニティへの広告宣伝等を用いることができる。

以上のようにして、ユーザに対し、新版ゲームプログラム４０の存在を通知させることができる。図４（ｂ）に示すように、更新を希望するユーザは、ウェブブラウザ３１を介して配信用コンピュータ１０にアクセスし、新版ゲームプログラム４０への更新を要求する（Ｓ１２）。

図４（ｃ）に示すように、配信用コンピュータ１０は、ユーザの希望する新版のゲームプログラム４０（付随データ群も含まれる）を、通信ネットワークを介して、ユーザコンピュータ３０に向けて送信する（Ｓ１３）。また、新版のゲームプログラム４０と一緒に実行制御プログラム５０もセットにしてユーザコンピュータ３０に送信される（Ｓ１３）。新版のゲームプログラム４０及び実行制御プログラム５０は、ユーザコンピュータ３０の記憶装置に保存される。

新版のゲームプログラム４０及び実行制御プログラム５０には、専用のインストーラが付属している。インストーラにより、新版のゲームプログラム４０及び実行制御プログラム５０がユーザコンピュータ３０にインストールされる。実行制御プログラムが起動すると、図４（ｄ）に示すように、実行制御プログラム５０は、ネットワークアクセスの機能を呼び出して、認証用コンピュータ２０にア

クセスし、認証用コンピュータ２０との間で、ユーザ認証及び購入処理（課金処理）を行う（Ｓ１４）。ユーザ認証や課金処理を終えた後で、認証用コンピュータ２０は、ユーザコンピュータ３０の実行制御プログラム５０に向けて、暗号化された起動情報を送信する（Ｓ１５）。

実行制御プログラム５０は、暗号化された起動情報を解読して、デコードキーや起動引数等を取り出す。そして、実行制御プログラム５０は、ゲームプログラム４０をデコードして起動させる。これにより、ユーザは、新版のゲームプログラム４０を利用することができる。ゲームプログラム４０の実行状態は、実行制御プログラム５０により監視される。

図４（ｅ）に示すように、ユーザがゲームプレイを終了し、ゲームプログラム４０が終了すると、実行制御プログラム５０は、新版のゲームプログラム４０を削除することにより無力化させる（Ｓ１６）。

一例として、デコードされて実行可能な状態（起動ステートメントの入力により起動可能な状態）に置かれている新版のゲームプログラム４０のみを削除し、配信用コンピュータ１０から取得したデコード前の暗号化ファイルは、ユーザコンピュータ３０の記憶装置内に保存しておくことができる。

これにより、ユーザがゲームプログラム４０の再プレイを希望する場合は、認証用コンピュータ２０にアクセスしてオンラインによるユーザ認証を受け、認証用コンピュータ２０から起動情報を改めて取得するだけで足りる（Ｓ１７）。暗号化されたゲームプログラム４０を配信用コンピュータ１０から改めて取得する必要がないため、ダウンロードの手間がかからず、また通信ネットワークへの負担を軽減することができる。

このように、ゲームプログラム４０を再度プレイする場合は、ゲームプログラム４０の起動情報のみを再取得する方法が便利であるが、本発明はこれに限らず、デコード前の暗号化されたプログラムを配信用コンピュータ１０から再度取得す

るようにしてもよい。また、デコードされたプログラム本体４１のみを削除し、付随データ群４２をそのまま残してもよい。

次に、図５及び図６に基づいて、本システムの処理の詳細を説明する。図に示すフローチャートは、処理の大まかな流れを示すものであり、実際のプログラムとは相違する。

図５は、ユーザコンピュータ３０の記憶装置に格納された新版のゲームプログラム４０及び実行制御プログラム５０をインストール等する処理を示す。

ゲームプログラム４０及び実行制御プログラム５０は暗号化ファイルの状態でユーザコンピュータ３０に保存される。例えば、ユーザが、暗号化ファイルをマウスポインタで選択してダブルクリックする等のように、起動イベントを発生させると、インストーラが起動する（Ｓ２１）。

インストーラは、ユーザコンピュータ３０に更新すべき旧版のゲームプログラム４０Ａがインストール済であるか否かを判定する（Ｓ２２）。旧版のゲームプログラム４０Ａがインストールされていない場合は、例えば、「旧版のゲームがインストールされていません。処理を終了します。」等のような警告メッセージを画面に表示させて終了する（Ｓ２３）。

旧版のゲームプログラム４０Ａがユーザコンピュータ３０にインストールされている場合は（S22:YES)、新版のゲームプログラム４０及び実行制御プログラム５０を初めてインストールするのか否かを判定する（Ｓ２４）。新版ゲームプログラム４０及び実行制御プログラム５０が過去にインストールされている場合は、既にユーザ登録及び課金処理が完了しているものとみなすことができる。従って、Ｓ２４は、結果的に、既にユーザ登録及び課金処理が完了しているか否かを判定することになる。

初めてのインストールである場合は、ウェブブラウザ３１の機能を呼び出して認証用コンピュータ２０に接続し、ユーザに、ユーザ登録及び課金処理を行わせ

る（Ｓ２５，Ｓ２６）。

次に、インストーラは、実行制御プログラム５０のレジストリを判定し、実行制御プログラム５０が未だインストールされていない場合は、実行制御プログラム５０をインストールする（Ｓ２７）。インストーラは、旧版のゲームプログラム４０Ａを新版のゲームプログラム４０に置き換えて更新すべく、旧版のプログラム本体４１及び付随データ群４２を新版のプログラム本体４１及び付随データ群４２に書き換える（Ｓ２８，Ｓ２９）。そして、インストーラは、実行制御プログラム５０を起動させて処理を終了する（Ｓ３０）。

図６は、実行制御プログラム５０による実行制御処理及び認証用コンピュータ２０の処理等を示すフローチャートである。

起動された実行制御プログラム５０は、ユーザコンピュータ３０に固有のマシン情報、具体的には、MAC アドレスを取得する（Ｓ４１）。また、ユーザコンピュータ３０の内蔵タイマから現在時刻の情報を取得し、この時刻情報に基づいて暗号化キーを生成する（Ｓ４２）。

次に、実行制御プログラム５０は、ウェブブラウザ３１の機能を呼び出し（Ｓ４３）、通信ネットワークを介して認証用コンピュータ１０に接続し、認証用コンピュータ２０にログイン認証を要求する（Ｓ４４）。実行制御プログラム５０は、ユーザＩＤ、パスワード、MAC アドレス及び暗号化キーを認証用コンピュータ２０に送信する（Ｓ４４）。認証用コンピュータ２０は、ユーザ情報データベース２４を参照し、正当なユーザであるか否かを判断する（Ｓ６１）。

正当なユーザであると認められた場合、認証用コンピュータ２０は、ユーザが利用可能なゲームプログラムの一覧データを作成し、ユーザコンピュータ３０に送信する（Ｓ６２）。ユーザが利用することができるゲームプログラムとしては、典型的には、そのユーザが購入しているゲームプログラムを挙げることができるが、これに限らず、例えば、ソフトウェア会社が無償で提供しているゲームプロ

グラム等を含めることもできる。

実行制御プログラム５０は、利用可能なゲームプログラムの一覧データを認証用コンピュータ２０から受信すると、ユーザコンピュータ３０のモニタディスプレイにゲームの一覧を表示させる（Ｓ４５）。この一覧メニューに基づいて、ユーザは、プレイを希望するゲームを選択する（Ｓ４６）。

認証用コンピュータ２０は、ゲーム情報データベース２５を参照して、ユーザが選択したゲームプログラムを起動させるために必要な起動情報を生成し、この起動情報を、Ｓ６１で取得した暗号化キー及び MAC アドレス等によって暗号化する（Ｓ６３）。認証用コンピュータ２０は、暗号化された起動情報をユーザコンピュータ３０の実行制御プログラム５０に送信する（Ｓ６４）。

実行制御プログラム５０は、暗号化された起動情報を認証用コンピュータ２０から受信すると（Ｓ４７）、この暗号化された起動情報を暗号化キー及び MAC アドレスによって解読する（Ｓ４８）。

次に、実行制御プログラム５０は、新版のゲームプログラム４０のレジストリ情報を取得し（Ｓ４９）、レジストリパスと起動引数とによって起動ステートメントを生成する（Ｓ５０）。

また、実行制御プログラム５０は、起動情報から取り出したデコードキーによって、暗号化された新版のゲームプログラム４０をデコードし、所定のドライブの所定のディレクトリに展開させる（Ｓ５１）。これにより、ゲームプログラム４０はデコードされて起動待ちの状態になる。

そして、実行制御プログラム５０は、Ｓ５０で生成した起動ステートメントによって、デコードされた新版のゲームプログラム４０を起動させる（Ｓ５２，Ｓ７０）。これにより、ユーザは、新版のゲームプログラム４０で遊ぶことができる（Ｓ７１）。

実行制御プログラム５０は、ゲームプログラム４０の実行状態を監視しており

（Ｓ５３）、ユーザがゲームを終えてゲームプログラム４０を終了させた場合には（Ｓ７２）、デコードされたプログラム本体４１を削除等することにより、ゲームプログラム４０を無力化し、処理を終了する（Ｓ５４）。

なお、ユーザが再びゲームプログラム４０で遊びたい場合は、再度認証用コンピュータ２０にアクセスしてオンラインによる認証を受け、起動情報を取得すればよい。

このように構成される本実施例によれば、ユーザコンピュータ３０にプログラムを格納させるダウンロード式のソフトウェア配信の場合でも、使用権を購入していない違法な使用を阻止することができる。

即ち、本実施例において、ゲームプログラム４０を起動させるには、使用する度毎に、実行制御プログラム５０を介してオンラインによる認証を行い、認証用コンピュータ２０から通信ネットワークを介して起動情報を取得する必要があるため、仮に、ゲームプログラム４０のみを単体で違法にコピーしても、違法にコピーされたゲームプログラム４０を単体で起動させることはできない。

また、実行制御プログラム５０はデバイスドライバのようにＯＳ側に近いプログラムとして構成されており、アプリケーションプログラムのように通常の方法では終了させることができない。従って、実行制御プログラム５０とゲームプログラム４０とを切り離して、ゲームプログラム４０のみを違法にコピーしたり持ち出したりすることができないようになっている。

本発明は、種々のビジネスに活用することができるであろう。例えば、過去に違法にコピーされて流通している旧版ゲームプログラムを、新版ゲームプログラムに更新させることにより、違法使用のユーザに正式に使用権を取得させて、正当なユーザへ変えることができる。違法なユーザを新版のゲームプログラムに乗り換えさせるためには、そのユーザの母国語に対応した付随データ群（ゲームシナリオや楽曲等）を用意したり、追加のシナリオ等を新しく用意したりして、ユ

ーザの更新意欲を刺激すればよい。

次に、図７～図１２を参照し、他の実施例を説明する。本実施例では、ゲームプログラムを記録媒体に固定して流通させる場合を例に挙げて説明する。本実施例では、本発明の範囲を減縮しない限りにおいて、前記実施例で述べた説明を適宜援用することができる。後述のように本実施例では、上記実施例と同様に、実行制御プログラム（本実施例のゲームマネージャ）によってゲームプログラムの実行を制御している。これに加えて、本実施例では、認証用コンピュータ（本実施例のＤＲＭコンピュータ）と実行制御プログラムとの間のオンライン認証を、定期的に実行可能としている。

図７は、本実施例によるソフトウェア実行制御システムの全体概要を示す説明図である。本システムは、それぞれ後述するように、例えば、サプライヤコンピュータ１００と、ＤＲＭコンピュータ２００と、ユーザコンピュータ３００とを含めて構成することができる。

サプライヤコンピュータ１００は、例えば、プログラムプロダクトを生産するソフトウェアベンダーにより使用される。サプライヤコンピュータ１００は、ゲームプログラム４００を加工してＤＲＭ化プログラム７００に変換するＤＲＭ部１１０を備えている。ここで、ＤＲＭとは、Digital Rights Management の略称であり、ゲームプログラム等のディジタル化されたコンテンツの権利を管理することを意味する。本明細書において、ＤＲＭ化とは、ノンプロテクトのゲームプログラムに後述する独自のプロテクトを設定することにより、不正使用等に対する耐性を向上させることを意味する。

ＤＲＭ部１１０は、ゲームプログラム４００に、ゲームマネージャ５００及び監視プログラム６００を加えることにより、ゲームプログラム４００に独自のプロテクトを設定する。プロテクトされたゲームプログラム４００は、ＤＲＭ化プ

ログラム７００として、記録媒体ＲＭに記録され市場に流通する。ゲームマネージャ５００及び監視プログラム６００については、さらに後述する。

記録媒体ＲＭとしては、例えば、CD － ROM、DVD － ROM、光ディスク、ハードディスク、フレキシブルディスク、半導体メモリ、磁気テープ等のような種々の媒体を適宜用いることができる。ＤＲＭ化プログラム７００を圧縮して記録媒体ＲＭに記録してもよいし、ＤＲＭ化プログラム７００を圧縮することなく記録媒体ＲＭに記録してもよい。また、記録媒体ＲＭには、ＤＲＭ化プログラム７００をユーザコンピュータ３００にインストールさせるためのインストーラを記憶させることもできる。

ＤＲＭコンピュータ２００は、「管理コンピュータ」の一例である。ＤＲＭ化コンピュータ２００は、例えば「認証管理サーバ」等と呼ぶこともできる。ＤＲＭ化コンピュータ２００は、各ソフトウェアベンダー毎にそれぞれ設置してもよいし、複数のソフトウェアベンダーに対して１つだけ設置してもよい。

ＤＲＭコンピュータ２００は、ユーザコンピュータ３００上で稼働するゲームマネージャ５００との間で通信を行うことにより、ユーザ認証、起動情報の送信、及び継続実行の管理を行うものである。ＤＲＭコンピュータ２００は、認証部２１０と、起動情報送信部２２０と、継続実行管理部２３０とを備えている。

また、ＤＲＭコンピュータ２００は、ユーザ情報データベース２４０と、ゲーム情報データベース２５０と、監視状況データベース２６０とを利用することができる。なお、ＤＲＭコンピュータ２００は、物理的に単一のコンピュータから構成されている必要はなく、複数のコンピュータの協働動作によって実現されてもよい。

認証部２１０は、前記実施例の認証部２１と同様に、例えば、ユーザＩＤ、パスワード（図中「ＰＷ」）ゲームマネージャ５００から送信される認証用データに基づいて、ユーザ認証を行うものである。起動情報送信部２２０は、前記実施例

の起動情報送信部２３と同様に、例えば、ゲームマネージャ５００がゲームプログラム４００をデコードして起動可能状態に置くために必要な情報を、ゲームマネージャ５００に送信するものである。

継続実行管理部２３０は、ゲームマネージャ５００との間で所定時間毎に通信を行うことにより、ゲームプログラム４００の実行継続の可否を管理するものである。詳細はさらに後述するが、継続実行管理部２３０は、ゲームマネージャ５００から送信されたセッションＩＤと予め保持されているセッションＩＤとを比較し、両者が一致する場合は、ゲームプログラム４００の実行継続を許可する。逆に、継続実行管理部２３０は、両セッションＩＤが一致しない場合、ゲームプログラム４００の強制終了をゲームマネージャ５００に対して指示する。

ユーザコンピュータ３００は、前記実施例のユーザコンピュータ３と同様に、例えば、パーソナルコンピュータや携帯情報端末、携帯電話等として構成可能なものである。ユーザコンピュータ３００は、ＣＰＵ、メモリ、補助記憶装置、ＯＳ、各種デバイスドライバ等のように、ハードウェア資源及びソフトウェア資源を必要に応じて備えることができる。ゲームプログラム４００と、ゲームマネージャ５００と、監視プログラム６００とは、ユーザコンピュータ３００の有するハードウェア資源及びソフトウェア資源を適宜利用することができる。

記録媒体ＲＭの記憶内容をユーザコンピュータ３００に読み込ませ、所定のインストール処理を行うことにより、ユーザコンピュータ３００上でゲームプログラム４００，ゲームマネージャ５００及び監視プログラム６００がそれぞれ実行される。正当な権限を有するユーザにとって、ゲームマネージャ５００はゲームプログラム４００を起動させるためのランチャープログラムとして作用する。しかし、ゲームマネージャ５００は、単なるランチャープログラムではなく、ゲームプログラム４００の作動を制御する。また、ゲームマネージャ５００は、ゲームプログラム４００及び監視プログラム６００の動作状態をそれぞれ監視し、い

ずれか一方の監視対象が動作を停止した場合は、他方の監視対象及び自身の動作を停止させる。

監視プログラム６００は、ゲームプログラム４００及びゲームマネージャ５００の動作状態をそれぞれ監視し、いずれか一方の監視対象が動作を停止した場合は、他方の監視対象及び自身の動作を停止させる。正当なユーザは、監視プログラム６００の存在を意識せずに、ゲームプログラム４００を使用することができる。

図８は、各データベース２４０～２６０の一例を示す説明図である。図８（ａ）に示すように、ユーザ情報データベース２４０は、例えば、ユーザＩＤと、パスワードと、MAC アドレスと、セッションＩＤと、その他の情報とを対応付けて管理することができる。後述のように、セッションＩＤは、継続実行を許可するか否かを判定するために用いられる情報である。即ち、最初に認証されたユーザコンピュータ３００とは別のユーザコンピュータを使用してゲームプログラム４００が不正に実行されるのを防止するために、ゲームマネージャ５００とＤＲＭコンピュータ２００とは定期的に通信を行う。この際に、ゲームマネージャ５００から受信したセッションＩＤと、ユーザ情報データベース２４０に登録されているセッションＩＤとの比較が行われ、セッションＩＤが一致する場合にのみゲームプログラム４００の実行継続が許可されるようになっている。なお、図２（ａ）に示すユーザ情報データベース２４と同様に、１つのユーザＩＤに複数の MAC アドレスを対応付けることもできる。

図８（ｂ）に示すように、ゲーム情報データベース２５０は、例えば、ゲームＩＤと、ゲーム名と、ゲーム情報と、デコードキー（アクティベイトキー）と、起動引数と、報告モードとを対応付けて管理することができる。ここで、報告モードとは、ゲームマネージャ５００からＤＲＭコンピュータ２００への定期的な報告の頻度に関する方針を設定する情報である。報告モードは、例えば、ゲーム

プログラム４００の提供者（ソフトウェアベンダー）が設定することができる。

ここで、報告モードとしては、例えば、ゲームプログラム４００を最初に起動した時だけＤＲＭコンピュータ２００に報告するモードと、ゲームプログラム４００を起動させる度にＤＲＭコンピュータ２００に報告するモードと、監視効率を優先して可能な限り短周期でＤＲＭコンピュータ２００に報告するモードと、ＤＲＭコンピュータ２００の負荷低減を考慮して少ない頻度でＤＲＭコンピュータ２００に報告するモードと、を挙げることができる。

図８（ｃ）に示すように、監視状況データベース２６０は、例えば、ゲームプログラム４００を実行している各ユーザのユーザＩＤと、各ユーザコンピュータ３００からの報告周期と、次回の報告時期と、各ユーザが実行しているゲームプログラム４００のゲームＩＤと、ゲームスタート時刻とを対応付けて管理することができる。後述のように、次回の報告時期は、ＤＲＭコンピュータ２００の負荷状態や報告モード等に基づいて動的に制御される。

次に、図９～図１２に基づいて、本システムの動作を説明する。まず、図９は、本システムの起動時に行われる動作の概要を示すフローチャートである。

ゲームプログラム４００の利用を希望するユーザは、例えば、所望のゲームプログラム４００を象徴するゲームアイコンを選択し、起動を指示する。このユーザによる操作が検出されると、まず最初に、ゲームマネージャ５００が起動する（Ｓ１０１）。

ゲームマネージャ５００は、ユーザコンピュータ３００に固有のマシン情報の一例である MAC アドレスを取得し（Ｓ１０２）、この MAC アドレスを通信ネットワークＣＮを介して、ＤＲＭコンピュータ２００に送信する（Ｓ１０３）。

ＤＲＭコンピュータ２００は、ゲームマネージャ５００から受信した MAC アドレスを、ユーザ情報データベース２４０に登録する（Ｓ１２１，Ｓ１２２）。この時点では、MAC アドレスのみが判明しているだけであり、ユーザＩＤ等との

対応付けはされない。なお、MAC アドレスをユーザ情報データベース２４０に登録せずに、メモリに保持しておき、ユーザ認証が成功した場合に、ユーザＩＤやセッションＩＤ等と共に MAC アドレスをユーザ情報データベース２４０に登録してもよい。

ＤＲＭコンピュータ２００は、セッションＩＤを発行し、また、報告周期を設定する。最初に設定される報告周期には、予め設定された初期値を用いることができる。そして、ＤＲＭコンピュータ２００は、セッションＩＤと初回の報告周期とをゲームマネージャ５００に通知する（Ｓ１２３）。

ゲームマネージャ５００は、セッションＩＤ及び報告周期を受信すると（Ｓ１０４）、これらの情報をユーザコンピュータ３００のメモリに格納して保持する。次に、ゲームマネージャ５００は、ユーザからユーザＩＤ及びパスワードが入力されたか否かを判定する（Ｓ１０５）。例えば、ユーザがゲームアイコンを選択操作したときに、ユーザＩＤ及びパスワードの入力を求める画面を表示させることにより、ユーザにユーザＩＤ及びパスワードの入力を促すことができる。

ゲームマネージャ５００は、ユーザＩＤ及びパスワードの入力を確認すると(S105：YES)、入力されたユーザＩＤ及びパスワードと、ユーザが実行を希望するゲームプログラム４００のゲームＩＤとをＤＲＭコンピュータ２００に送信する（Ｓ１０６）。

ＤＲＭコンピュータ２００は、ゲームマネージャ５００からユーザＩＤ、パスワード及びゲームＩＤを受信すると（Ｓ１２４）、ユーザ情報データベース２４０を参照し、ユーザ認証を行う（Ｓ１２５）。予め登録されているユーザＩＤ及びパスワードと、ゲームマネージャ５００から受信したユーザＩＤ及びパスワードとが一致する場合（S125：YES)、ユーザ認証は成功する。ＤＲＭコンピュータ２００は、ユーザＩＤ、パスワード、MAC アドレス等を対応付けてユーザ情報データベース２４０に登録する（Ｓ１２７）。逆に、ユーザＩＤまたはパスワードのい

ずれか一方が一致しない場合（S125：NO）、ユーザ認証は失敗し、エラー処理が行われる（Ｓ１２６）。エラー処理としては、例えば、「ＩＤまたはパスワードが違います」等のメッセージをユーザコンピュータ３００の画面に表示させることが考えられる。また、例えば、所定回数以上ユーザ認証が失敗した場合は、ゲームプログラム４００の起動をロックさせることも可能である。なお、ユーザ認証の情報としては、ユーザＩＤ及びパスワードに限らず、例えば、声紋、指紋、虹彩等の生体情報を採用してもよい。

ＤＲＭコンピュータ２００は、ユーザ認証の成功によって、ユーザが希望するゲームプログラム４００の実行許可を決定する（Ｓ１２８）。ＤＲＭコンピュータ２００は、実行を許可したゲームプログラム４００をゲームマネージャ５００が起動できるようにするための情報を生成して暗号化する（Ｓ１２９）。このゲーム起動用の情報としては、例えば、ファイル名等の実行情報やアクティベイトキー等を挙げることができる。ＤＲＭコンピュータ２００は、これら実行情報及びアクティベイトキーを、例えば、セッションＩＤやユーザ情報（MACアドレス等）を用いて暗号化し、この暗号化された情報をゲームマネージャ５００に送信する（Ｓ１３０）。

ゲームマネージャ５００は、ＤＲＭコンピュータ２００から暗号化情報を受信すると（Ｓ１０７）、暗号化情報を解凍して（Ｓ１０８）、アクティベイトキー及び実行情報を取得する（Ｓ１０９）。ＤＲＭコンピュータ２００が使用する暗号アルゴリズムは、ゲームマネージャ５００にとって既知であり、解凍に必要な情報はユーザコンピュータ３００側にも存在するので、暗号化情報を解凍することができる。

ゲームマネージャ５００は、入手したアクティベイトキーによってゲームプログラム４００をデコードし、このデコードしたゲームプログラム４００をユーザコンピュータ３００のメモリに格納させる（Ｓ１１０）。

即ち、記録媒体ＲＭを用いてゲームプログラム４００をユーザコンピュータ３００にインストールした場合、ゲームプログラムは、例えば、ユーザコンピュータ３００の補助記憶装置にエンコードされた状態で記憶される。このエンコードされた状態では、ゲームプログラム４００を起動させることはできない。ゲームマネージャ５００がＤＲＭコンピュータ２００からアクティベイトキーを取得してゲームプログラム４００をデコードし、ユーザコンピュータ３００のメモリに置いた時点で、ゲームプログラム４００は起動可能となる。ここで、注意すべき点は、デコードされたゲームプログラム４００（実行体プログラム）は、ファイルとして保存されるのではなく、メモリ内にのみ存在する点である。ゲームプログラム４００の終了時には、メモリ内のプログラムが消去されるため、再度ゲームをプレイをする場合は、ゲームマネージャ５００を介して再びユーザ認証やアクティベイトキーの取得等を行う必要がある。

そして、ゲームマネージャ５００は、実行情報に基づいて、ユーザコンピュータ３００のメモリに置かれたゲームプログラム４００を起動させる（Ｓ１１１）。これにより、ユーザは、ゲームプログラム４００を実行させて遊ぶことができるようになる。また、ゲームマネージャ５００は、ゲームプログラム４００の起動と同時に（物理的に厳密な意味で同時でなくてもよい）、監視プログラム６００を起動させる（Ｓ１１２）。監視プログラム６００の動作については、さらに後述する。

次に、ゲームプログラム４００の実行継続を制御するための監視処理について、図１０に基づき説明する。

ゲームマネージャ５００は、起動時にＤＲＭコンピュータ２００から設定された報告周期を参照する（Ｓ１４１）。ゲームマネージャ５００は、ユーザコンピュータ３００が有するタイマ機能等を利用することにより、ＤＲＭコンピュータ２００から予め設定された報告時期が到来したか否かを判定する（Ｓ１４２）。

報告時期が到来した場合（S142：YES)、ゲームマネージャ５００は、ＤＲＭコンピュータ２００から設定されたセッションＩＤをユーザコンピュータ３００のメモリから読出し（Ｓ１４３)、この読み出したセッションＩＤをＤＲＭコンピュータ２００に送信する（Ｓ１４４)。

ＤＲＭコンピュータ２００は、ゲームマネージャ５００からセッションＩＤを受信すると（Ｓ１６１)、ユーザ情報データベース２４０を参照する。ＤＲＭコンピュータ２００は、ユーザ情報データベース２４０に登録されている発行済セッションＩＤと、ゲームマネージャ５００から受信したセッションＩＤとを比較し、両者が一致するか否かを判定する（Ｓ１６３)。なお、ゲームマネージャ５００からＤＲＭコンピュータ２００に対して、セッションＩＤのみを送信してもよいし、あるいは、セッションＩＤに加えて、例えば、ユーザＩＤ等のユーザ情報の全部または一部を含めることもできる。さらには、ユーザコンピュータ３００の環境情報（ＣＰＵ利用率やメモリ消費量等）を含めることも可能である。しかし、セッションＩＤに付加する情報が増大するほど、ユーザコンピュータ３００の負荷は増し、また、ネットワークトラフィックも増大する。

ゲームマネージャ５００から受信したセッションＩＤが予め登録されているセッションＩＤと一致しない場合（S163：NO)、ＤＲＭコンピュータ２００（継続実行管理部２３０）は、ゲームマネージャ５００に対して、ゲームプログラム４００の実行継続の禁止を通知する（Ｓ１６４)。両セッションＩＤが不一致の場合は、別のユーザコンピュータでゲームプログラム４００を実行等している場合、即ち、例えば、１つのユーザＩＤで同一のゲームプログラム４００を複数起動しているような場合である。そこで、両セッションＩＤが不一致の場合は、ゲームプログラム４００の強制終了をゲームマネージャ５００に指令する。

ゲームマネージャ５００から受信したセッションＩＤと予め登録されているセッションＩＤとが一致する場合（S163：YES)、ＤＲＭコンピュータ２００は、新

たな報告周期、即ち、次回の報告時期を算出する（Ｓ１６５）。この新たな報告周期の算出については、さらに後述するが、ＤＲＭコンピュータ２００の負荷状態等を考慮して決定される。

両セッションＩＤが一致する場合、ＤＲＭコンピュータ２００は、新たに算出された報告周期と実行継続の許可とをゲームマネージャ５００に通知する（Ｓ１６６）。

ゲームマネージャ５００は、ＤＲＭコンピュータ２００から実行継続の可否について応答を受信する（Ｓ１４５）。ゲームマネージャ５００は、ゲームプログラム４００の実行継続が許可された場合（S146：YES）、新たに設定された報告周期をユーザコンピュータ３００のメモリに保存して、Ｓ１４１に戻り、報告時期の到来を待つ。

逆に、ＤＲＭコンピュータ２００から実行継続が禁止された場合（S146：NO）、ゲームマネージャ５００は、実行中のゲームプログラム４００を強制的に終了させる（Ｓ１４７）。そして、ゲームマネージャ５００は、監視プログラム６００を終了させた後（Ｓ１４８）、自身も終了させる（Ｓ１４９）。

上述のように、ゲームマネージャ５００は、ＤＲＭコンピュータ２００との間で簡易な認証を定期的に行う。これにより、例えば、同一のユーザＩＤ及びパスワードを用いてゲームプログラム４００を複数起動させるような不正な利用を防止することができる。

図１１は、報告周期の設定処理を示すフローチャートである。図１０中のＳ１６５の内容を具体化した一例である。ＤＲＭコンピュータ３００（詳しくは、継続実行管理部２３０）は、ゲームマネージャ５００からセッションＩＤを受信した時刻を参照する（Ｓ１８１）。次に、ゲームマネージャ５００は、このセッションＩＤの受信に関連付けられていた報告周期を参照する（Ｓ１８２）。

ゲームマネージャ５００は、セッションＩＤの受信時刻と予め設定されていた

報告周期とのずれを算出する。例えば、セッションＩＤの受信予定時刻よりも実際の受信時刻が遅れている場合は、通信ネットワークＣＮの混雑によるパケット到着の遅れや、ＤＲＭコンピュータ３００の負荷増大による応答性能の低下等を原因として挙げることができる。

ＤＲＭコンピュータ２００は、自身の現在の負荷状態を検出する（Ｓ１８４）。この負荷状態としては、例えば、現在プレイ中のユーザ数、即ち、オンラインによる定期的な認証処理を行うべきゲームマネージャ数を挙げることができる。これに加えて、例えば、例えば、ＣＰＵ利用率、メモリ消費量、データ入出力処理速度（Ｉ／Ｏ速度）等を検出してもよい。

ＤＲＭコンピュータ２００は、現在の負荷状態に基づいて、将来の負荷状態を予測する（Ｓ１８５）。即ち、ＤＲＭコンピュータ２００は、ゲームマネージャ５００の報告周期を現在値に維持した場合に、次の報告時期におけるＤＲＭコンピュータ２００の負荷状態を予測する。具体的には例えば、もしも仮に、現在の報告周期が「１時間」に設定されている場合、現在時刻から１時間後にオンライン認証を行うユーザ数（ゲームマネージャ数）は、監視状況データベース２６０により把握できる。

次に、ＤＲＭコンピュータ２００は、実行中のゲームプログラム４００に予め設定されている報告モードを参照する（Ｓ１８６）。ゲームプログラム４００に関連付けられる報告モードは、記録媒体ＲＭの流通後でも変更可能である。例えば、サプライヤコンピュータ１００からＤＲＭコンピュータ２００に対して、ゲームＩＤ及び新たな報告モードを通知し、ゲーム情報データベース２５０の更新を要求すればよい。

最後に、ＤＲＭコンピュータ２００は、例えば、報告モードと、セッションＩＤの受信予定時刻と実際の受信時刻との時間的なずれ量と、将来の予測負荷状態とに基づいて、監視効率が最大となるように、新たな報告周期を算出する（Ｓ１

８７）。

例えば、新作の人気ゲームプログラムが発売された当初は、そのゲームプログラムのユーザ数が急激に増大する。従って、オンラインによる周期的な簡易認証を行うＤＲＭコンピュータ２００の負荷は増大する。報告周期を短く設定するほど、不正使用に対するセキュリティ性が向上するが、その反面、ＤＲＭコンピュータ２００の負荷も増大する。セキュリティ性を重視するあまりに報告周期を短く設定すると、ＤＲＭコンピュータ２００の応答性が低下したり、機能停止を招く可能性がある。そこで、新作人気ゲームの発売当初等のように、一時的に負荷が増大するような場合は、報告周期が長くなるように制御する。

このように、ＤＲＭコンピュータ２００は、例えば、監視優先モードの場合、機能停止を招かない範囲で最大限のセキュリティ性が得られるように、報告周期（監視タイミング）を設定することができる。一方、負荷軽減モードの場合、ＤＲＭコンピュータ２００は、最低限のセキュリティ性を維持できる程度に報告周期を設定することができる。

以上は一例であって、負荷状態の予測や報告周期の設定等には、種々のアルゴリズムを取り入れることができる。

次に、図１２は、ゲームマネージャ５００及び監視プログラム６００による相互監視の処理を示すフローチャートである。本実施例では、ゲームマネージャ５００と監視プログラム６００とは、それぞれ共通の監視対象としてゲームプログラム４００の動作状態を監視するほか、お互いも監視対象として定期的に監視している。ＤＲＭコンピュータ２００とゲームマネージャ５００との間の定期的なオンライン認証を外部からの監視とすれば、ゲームマネージャ５００及び監視プログラム６００による相互監視を内部での監視と位置づけることができる。

ゲームマネージャ５００の監視処理について先に説明すると、ゲームマネージャ５００は、予め設定された監視時期が到来したか否かを判定する（Ｓ２０１）。

監視時期は比較的短周期に設定するのが好ましい。監視時期が到来すると（S201：YES）、ゲームマネージャ５００は、監視プログラム６００の動作状態を確認し（Ｓ２０３）、監視プログラム６００が正常に動作しているか否かを判定する（Ｓ２０３）。

監視プログラム６００が正常に動作している場合（S203：YES）、次に、ゲームマネージャ５００は、ゲームプログラム４００の動作状態を確認し（Ｓ２０４）、ゲームプログラム４００が正常に動作しているか否かを判定する（Ｓ２０５）。ゲームプログラム４００も正常に動作している場合（S205：YES）、ゲームマネージャ５００は、次の監視時期が到来するまで待機する（Ｓ２０１）。

一方、監視プログラム６００が動作を停止していた場合（S203：NO）、あるいは、ゲームプログラム４００が動作を停止していた場合（S205：NO）、ゲームマネージャ５００は、強制停止処理（Ｓ２０６～Ｓ２０８）に移行する。

即ち、ゲームマネージャ５００は、ゲームプログラム４００及び監視プログラム６００の両方の動作を停止させた後（Ｓ２０６，Ｓ２０７）、ゲームマネージャ自身も停止させる（Ｓ２０８）。ゲームプログラム４００の動作が停止された場合は、デコードされたゲームプログラム４００は、ユーザコンピュータ３００のメモリから直ちに消去ないし破壊される。

なお、既に停止しているプログラムについては、改めて停止を命令する必要がない。例えば、ゲームプログラム４００の動作停止が確認されて強制停止処理に移行した場合は、ゲームプログラム４００の動作停止を改めて指示する必要はない。同様に、監視プログラム６００の動作停止が確認されて強制停止処理に移行した場合は、監視プログラム６００の動作停止を改めて指示する必要はない。しかし、念のために、ゲームプログラム４００及び監視プログラム６００の両方に動作停止を命じてもよい。

監視プログラム６００の処理も同様である。監視プログラム６００は、監視時

期が到来すると（S221：YES)、ゲームマネージ５００及びゲームプログラム４００の動作状態をそれぞれ監視し（Ｓ２２２～Ｓ２２５)、いずれか一方が動作を停止していた場合は（S223：NO、または S225：NO)、強制停止処理に移行し、全てのプログラムを停止させる（Ｓ２２６～Ｓ２２８)。

このように、ゲームマネージャ５００及び監視プログラム６００という複数の動作監視用プログラムが、ゲームプログラム４００の動作状態を監視すると共に、それぞれお互いをも監視するため、ゲームプログラム４００の動作停止をより確実に検出することができる。また、一方の動作監視用プログラムが意図的に停止された場合でも、他方の監視用プログラムが全体のシャットダウンを行うため、ユーザコンピュータ３００のメモリに展開されたゲームプログラム４００が不正にコピーされるのを未然に防止することができる。

以上詳述した通り、本実施例によれば、ゲームプログラム４００の作動を制御するゲームマネージャ５００とライセンス認証を行うＤＲＭコンピュータ２００との間で、定期的なオンライン認証を行うため、不正使用に対する耐久性を高めることができる。

また、この定期的なオンライン認証は、セッションＩＤの比較により行われるため、比較的簡易な処理で済む。従って、コンピュータ負荷を増大させずに、簡易な認証を比較的短周期で行うことができ、長時間にわたってセキュリティ性を維持することも可能となる。

さらに、オンラインによる簡易認証を行うタイミング（報告周期）を、ＤＲＭコンピュータ２００の負荷状態等に基づいて動的に制御するため、ネットワークトラフィックやコンピュータ負荷等を考慮して、より高いセキュリティ性を実現することができる。

また、ゲームマネージャ５００及び監視プログラム６００という、２種類のそれぞれ独立した動作監視用プログラムを用意し、ゲームプログラム４００の動作

状態のみならず、それぞれお互いの監視をも行い、ゲームプログラム４００，ゲームマネージャ５００，監視プログラム６００のいずれか１つでも動作を停止した場合は、残りの２つのプログラムの動作も停止させ、ゲームプログラム４００を消去等して無力化する構成のため、メモリに展開されたゲームプログラム４００を不正に読み出してコピー等する行為を阻止して、信頼性をより高めることができる。

次に、図１３は、本発明のさらに別の実施例を示す。本実施例は、第１実施例において、複数の監視用プログラムによる相互監視と、認証用コンピュータとの間の定期的なオンライン認証とを実現させるものである。

本実施例では、配信用コンピュータ１０からユーザコンピュータ３０に向けて、ゲームプログラム４０と実行制御プログラム５０Ａと監視プログラム６０とが配信される。

実行制御プログラム５０Ａは、上述した実行制御プログラム５０の構成及び作用に加えて、上述したゲームマネージャ５００が実行する定期的な簡易オンライン認証機能と監視機能とを備えている。また、監視プログラム６０は、上述した監視プログラム６００と同様の監視機能を備えている。

実行制御プログラム５０Ａは、最初のユーザ認証によりゲームプログラム４０のデコード等を行う。また、実行制御プログラム５０Ａは、認証用コンピュータ２０に対して定期的にセッションＩＤを送信することにより、ゲームプログラム４０の実行中においてもユーザ認証を行う。実行制御プログラム５０Ａは、ユーザ認証が成功した場合はゲームプログラム４０の継続的な実行を許可し、ユーザ認証が失敗した場合はゲームプログラム４０を強制的に終了させる。

また、実行制御プログラム５０Ａと監視プログラム６０とは、共にゲームプログラム４０の起動状態を監視していると共に、お互い同士もそれぞれ監視してい

る。そして、ゲームプログラム４０，実行制御プログラム５０Ａ，監視プログラム６０のうちいずれか１つのプログラムが終了した場合は、実行制御プログラム５０Ａまたは監視プログラム６０がこれを検出し、残りのプログラム及び自分自身を終了させる。

なお、上述した本発明の各実施例は、本発明の説明のための例示であり、本発明の範囲を実施例にのみ限定する趣旨ではない。当業者は、本発明の要旨を逸脱することなしに、他の様々な態様で本発明を実施できる。

請 求 の 範 囲

1． ユーザコンピュータにインストールされた第１のソフトウェアを第２のソフトウェアに更新させるソフトウェア実行制御システムであって、

エンコードされた前記第２のソフトウェア及び該第２のソフトウェアの実行を制御するための実行制御プログラムを前記ユーザコンピュータに通信ネットワークを介して配信する配信部と、

前記ユーザコンピュータにインストールされた前記実行制御プログラムからの要求によってユーザ認証を行い、正当なユーザであると確認した場合には、前記第２のソフトウェアをデコードして起動させるために必要な所定の情報を前記通信ネットワークを介して前記実行制御プログラムに送信する認証部と、

を備え、

前記第２のソフトウェアは前記実行制御プログラムから渡される起動情報のみで起動可能に構成されており、

前記実行制御プログラムは、

（１）前記認証部から受信した前記所定の情報に基づいて前記エンコードされた第２のソフトウェアをデコードして前記第１のソフトウェアに置き換え、

（２）前記所定の情報に基づいて起動情報を生成することにより、前記第２のソフトウェアを起動させ、

（３）前記第２のソフトウェアの実行が終了された場合には、前記第２のソフトウェアを無力化させるように構成されているソフトウェア実行制御システム。

2． 前記実行制御プログラムは、複数種類の第２のソフトウェアに対応可能に構成されており、

前記認証部が前記実行制御プログラムに送信する前記所定の情報には、起動さ

せる第２のソフトウェアの格納先アドレス情報と起動引数と第２のソフトウェアをデコードするためのデコードキー情報とが含まれている請求項１に記載のソフトウェア実行制御システム。

３．　前記実行制御プログラムは、前記ユーザコンピュータに固有のマシン情報と暗号化キー情報とを含む認証用情報を前記認証部に送信し、

前記認証部は、少なくとも前記マシン情報に基づいてユーザ認証を行い、正当なユーザであると確認した場合には、前記所定の情報を前記暗号化キー情報で暗号化して前記通信ネットワークを介して前記実行制御プログラムに送信するものであり、

かつ、前記認証部には、前記マシン情報を複数個登録可能である請求項１に記載のソフトウェア実行制御システム。

４．　前記認証部は、正当なユーザであると確認した場合には、該ユーザが起動可能な第２のソフトウェアの一覧データを前記ユーザコンピュータに送信し、

前記一覧データから選択された第２のソフトウェアに関する前記所定の情報を前記通信ネットワークを介して前記実行制御プログラムに送信するものである請求項１に記載のソフトウェア実行制御システム。

５．　前記実行制御プログラムは、

前記ユーザコンピュータに固有のマシン情報を取得する機能と、

暗号化キー情報を生成する機能と、

前記認証部にユーザ認証を要求し、少なくとも前記マシン情報及び前記暗号化キー情報を前記認証部に送信する機能と、

前記認証部から受信した起動可能な第２のソフトウェアの一覧データからいず

れか１つの第２のソフトウェアをユーザに選択させ、選択された第２のソフトウェアを前記認証部に通知する機能と、

前記選択された第２のソフトウェアの前記ユーザコンピュータにおける格納先アドレス情報と起動引数とデコードキー情報とを少なくとも前記暗号化キー情報により暗号化してなる所定の情報を受信する機能と、

前記暗号化された所定の情報を少なくとも前記暗号化キー情報により解読する機能と、

前記解読されたデコードキー情報により前記ユーザコンピュータ内の第２のソフトウェアをデコードさせる機能と、

前記解読された起動引数及び前記格納先アドレス情報に基づいて、前記起動情報を生成する機能と、

前記生成された起動情報によって前記デコードされた第２のソフトウェアを起動させる機能と、

前記起動された第２のソフトウェアの実行状態を監視し、該第２のソフトウェアの実行が終了した場合は、前記第２のソフトウェアを無力化させる機能と、

を前記ユーザコンピュータ上に実現させるものである請求項１に記載のソフトウェア実行制御システム。

６．　前記第２のソフトウェアは、プログラムと付随データ群とを含んでなり、前記プログラム又は前記付随データ群の少なくともいずれか一方を更新させるものである請求項１に記載のソフトウェア実行制御システム。

７．　前記ユーザコンピュータにインストールされている前記第１のソフトウェアは、前記第２のソフトウェアに置換されるまでは、前記認証部による認証を受けることなく実行可能である請求項１に記載のソフトウェア実行制御システム。

8． 前記実行制御プログラムは、前記第２のソフトウェアの実行が終了した場合は、前記第２のソフトウェアの全部又は一部を削除することにより無力化させるものである請求項１に記載のソフトウェア実行制御システム。

9． 前記第２のソフトウェアは、プログラムと付随データ群とを含んでなり、前記実行制御プログラムは、前記第２のソフトウェアの実行が終了した場合は、前記第２のソフトウェアのエンコードデータは保存しつつ、前記デコードされた第２のソフトウェアのうち前記プログラムのみを無力化させるものである請求項１に記載のソフトウェア実行制御システム。

１０． 前記実行制御プログラムは、前記第２のソフトウェアとは別に強制終了させることができないプログラムとして構成されている請求項１に記載のソフトウェア実行制御システム。

１１． 前記配信部と前記認証部とは、それぞれ別体のコンピュータ上に実現されている請求項１に記載のソフトウェア実行制御システム。

１２．前記実行制御プログラムは、前記第２のソフトウェアの実行中に、前記認証部との間で定期的または不定期なユーザ認証を行うものであり、このユーザ認証が失敗した場合は前記第２のソフトウェアを強制的に終了させる請求項１に記載のソフトウェア実行制御システム。

１３．前記第２のソフトウェアの実行中に行われる定期的または不定期なユーザ認証は、少なくとも予測される将来の認証用コンピュータの負荷状態を考慮し

て、可変に制御可能である請求項１２に記載のソフトウェア実行制御システム。

１４．前記配信部は、前記第２のソフトウェア及び前記実行制御プログラムと共に監視プログラムを前記ユーザコンピュータに配信し、

前記監視プログラムは、前記第２のソフトウェア及び前記実行制御プログラムの動作状態をそれぞれ監視し、前記第２のソフトウェアまたは前記実行制御プログラムのいずれか一方が動作を停止した場合は、前記第２のソフトウェア及び前記実行制御プログラムをそれぞれ停止させ、自身も停止させるものであり、

前記実行制御プログラムは、前記第２のソフトウェア及び前記監視プログラムの動作状態をそれぞれ監視し、前記第２のソフトウェアまたは前記監視プログラムのいずれか一方が動作を停止した場合は、前記第２のソフトウェア及び前記監視プログラムをそれぞれ停止させ、自身も停止させるものである請求項１に記載のソフトウェア実行制御システム。

１５．ユーザコンピュータにインストールされた第１のソフトウェアを第２のソフトウェアに更新し、この第２のソフトウェアの実行を制御する実行制御プログラムであって、

外部の認証部と通信ネットワークを介して通信し、ユーザ認証を求める第１の機能と、

前記認証部から受信した所定の情報に基づいて、前記第２のソフトウェアを起動させるための起動情報を生成する第２の機能と、

前記認証部から受信した所定の情報に基づいて、前記第２のソフトウェアをデコードさせる第３の機能と、

前記ユーザコンピュータに既にインストールされている更新前のソフトウェアを前記デコードされた第２のソフトウェアに置き換える第４の機能と、

前記生成された起動情報によって前記第２のソフトウェアを起動させる第５の機能と、

前記第２のソフトウェアの実行状態を監視し、前記第２のソフトウェアの実行が終了した場合は、前記第２のソフトウェアを無力化させる第６の機能と、

を前記ユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

１６．　前記第２のソフトウェアは、プログラムと付随データ群とを含んでなり、

前記第４の機能は、前記プログラム又は前記付随データ群の少なくともいずれか一方を置き換えるものである請求項１５に記載のソフトウェアの実行制御プログラム。

１７．　前記ユーザコンピュータに既にインストールされている更新前のソフトウェアは、前記第４の機能によって前記第２のソフトウェアに置換される前は、前記認証部による認証を受けることなく実行可能である請求項１６に記載のソフトウェアの実行制御プログラム。

１８．　前記第６の機能は、前記第２のソフトウェアの実行が終了した場合は、前記第２のソフトウェアの全部又は一部を削除することにより無力化させるものである請求項１７に記載のソフトウェアの実行制御プログラム。

１９．　前記第２のソフトウェアは、プログラムと付随データ群とを含んでなり、

前記第６の機能は、前記第２のソフトウェアの実行が終了した場合は、前記第２のソフトウェアのエンコードデータは保存しつつ、前記デコードされた第２の

ソフトウェアのうち前記プログラムのみを無力化させるものである請求項１７に記載のソフトウェアの実行制御プログラム。

２０．　前記実行制御プログラムは、前記第２のソフトウェアとは別に強制終了させることができないプログラムとして構成されている請求項１５に記載のソフトウェアの実行制御プログラム。

２１．　ユーザコンピュータにインストールされたソフトウェアを第２のソフトウェアに更新し、この第２のソフトウェアの実行を制御する実行制御プログラムであって、

前記ユーザコンピュータに固有のマシン情報を取得する機能と、

暗号化キー情報を生成する機能と、

外部の認証部にユーザ認証を要求し、少なくとも前記マシン情報及び前記暗号化キー情報を前記認証部に送信する機能と、

前記認証部から受信した起動可能な第２のソフトウェアの一覧データからいずれか１つの第２のソフトウェアをユーザに選択させ、選択された第２のソフトウェアを前記認証部に通知する機能と、

前記選択された第２のソフトウェアの前記ユーザコンピュータにおける格納先アドレス情報と起動引数とデコードキー情報とを前記暗号化キー情報により暗号化してなる所定の情報を受信する機能と、

前記暗号化された所定の情報を少なくとも前記暗号化キー情報により解読する機能と、

前記解読されたデコードキー情報により前記ユーザコンピュータ内の第２のソフトウェアをデコードさせる機能と、

前記解読された起動引数及び前記格納先アドレス情報に基づいて、前記起動情

報を生成する機能と、

前記生成された起動情報によって前記デコードされた第２のソフトウェアを起動させる機能と、

前記起動された第２のソフトウェアの実行状態を監視し、該第２のソフトウェアの実行が終了した場合は、前記第２のソフトウェアを無力化させる機能と、

を前記ユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

２２．　ユーザコンピュータにインストールされている自由に使用可能な第１のソフトウェアを第２のソフトウェアに更新可能である旨をユーザに通知させるステップと、

前記第２のソフトウェアを配信する配信用コンピュータに前記ユーザコンピュータを通信ネットワークを介して接続させ、前記第２のソフトウェアへの更新を要求させるステップと、

前記配信用コンピュータから前記ユーザコンピュータにエンコードされた前記第２のソフトウェア及び該第２のソフトウェアの実行を制御するための実行制御プログラムを通信ネットワークを介して送信させるステップと、

前記ユーザコンピュータ上で起動した前記実行制御プログラムにより、前記ユーザコンピュータと認証用コンピュータとを通信ネットワークを介して接続させ、前記認証用コンピュータにユーザ認証を要求させるステップと、

前記ユーザ認証により正当なユーザであると認められた場合に前記認証用コンピュータから前記ユーザコンピュータに送信される所定の情報に基づいて、前記第２のソフトウェアをデコードするステップと、

前記認証用コンピュータから受信した前記所定の情報に基づいて、前記第２のソフトウェアを起動させるための起動情報を生成させるステップと、

前記生成された起動情報によって前記第２のソフトウェアを起動させるステッ

プと、

前記起動された第２のソフトウェアの実行を監視し、前記第２のソフトウェアの実行が終了した場合は、前記第２のソフトウェアを無力化させるステップと、

を含んでなるソフトウェアの更新方法。

２３．　第１のソフトウェアに置換される第２のソフトウェアと共にユーザコンピュータにインストールされる実行制御プログラムからの要求によってユーザ認証を行う認証部と、

前記認証部により正当なユーザであると確認された場合は、前記第２のソフトウェアをデコードして起動させるために必要な所定の情報を前記実行制御プログラムに送信する情報送信部と、

を備え、

前記第２のソフトウェアは前記実行制御プログラムから渡される起動情報のみで起動可能に構成されており、

前記実行制御プログラムは、

（１）前記認証部から受信した前記所定の情報に基づいて前記エンコードされた第２のソフトウェアをデコードして前記第１のソフトウェアに置き換え、

（２）前記所定の情報に基づいて起動情報を生成することにより、前記第２のソフトウェアを起動させ、

（３）前記第２のソフトウェアの実行が終了された場合には、前記第２のソフトウェアを無力化させるように構成されているコンピュータ。

２４．　アプリケーションソフトウェア及び監視プログラムと共にユーザコンピュータにインストールされる実行制御プログラムと通信を行うことにより、前記実行制御プログラムの動作を制御する管理用コンピュータであって、

前記実行制御プログラムからの要求に基づいてユーザ認証を行う認証部と、

前記認証部により正当なユーザであると確認された場合は、前記実行制御プログラムが前記アプリケーションソフトウェアを起動させるために必要な第１の情報を前記実行制御プログラムに送信する情報送信部と、

所定の時期に前記実行制御プログラムとの間で行われる継続確認通信に基づいて、前記アプリケーションソフトウェアの実行継続を許可するか否かを管理する継続実行管理部と、を備えた管理用コンピュータ。

２５．前記継続実行管理部は、前記継続確認通信によって前記実行制御プログラムから取得される第１の識別情報と前記ユーザ認証に予め関連付けられている第２の識別情報とを比較し、両方の識別情報が対応する場合は、前記実行制御プログラムに対して前記アプリケーションソフトウェアの実行継続を許可し、前記各識別情報が対応していない場合は、前記実行制御プログラムに対して前記アプリケーションソフトウェアの実行継続を禁止させる請求項２４に記載の管理用コンピュータ。

２６．　前記継続実行管理部は、前記第２の識別情報に対応する前記第１の識別情報を予め前記実行制御プログラムに設定させる請求項２５に記載の管理用コンピュータ。

２７．　前記継続実行管理部は、前記所定の時期を前記実行制御プログラムに予め設定し、この予め設定された所定の時期が到来した場合は、前記実行制御プログラムから前記継続実行管理部に対して前記継続確認通信を行わせる請求項２４に記載の管理用コンピュータ。

２８．　前記継続実行管理部は、前記所定の時期を可変に設定可能である請求項２４に記載の管理用コンピュータ。

２９．　前記継続実行管理部は、少なくとも予測される将来の負荷状態を考慮して、前記所定の時期を可変に設定可能である請求項２８に記載の管理用コンピュータ。

３０．　前記監視プログラムは、前記アプリケーションソフトウェア及び前記実行制御プログラムの動作状態をそれぞれ監視し、前記アプリケーションソフトウェアまたは前記実行制御プログラムのいずれか一方が動作を停止した場合は、前記アプリケーションソフトウェア及び前記実行制御プログラムをそれぞれ停止させ、自身も停止させるものであり、

前記実行制御プログラムは、前記アプリケーションソフトウェア及び前記監視プログラムの動作状態をそれぞれ監視し、前記アプリケーションソフトウェアまたは前記監視プログラムのいずれか一方が動作を停止した場合は、前記アプリケーションソフトウェア及び前記監視プログラムをそれぞれ停止させ、自身も停止させるものである請求項２４に記載の管理用コンピュータ。

３１．　アプリケーションソフトウェアが実行されるユーザコンピュータと、前記アプリケーションソフトウェアの実行を管理する管理用コンピュータとを備えたソフトウェア実行制御システムであって、

前記ユーザコンピュータには、

前記アプリケーションソフトウェアの実行を制御するための実行制御部と、

前記アプリケーションソフトウェア及び前記実行制御プログラムの動作を監視するための監視部とが設けられ、

前記管理用コンピュータには、

前記実行制御プログラムからの要求に基づいてユーザ認証を行う認証部と、

前記認証部により正当なユーザであると確認された場合は、前記実行制御部が前記アプリケーションソフトウェアを起動させるために必要な第１の情報を前記実行制御部に送信する情報送信部と、

所定の時期に前記実行制御部との間で行われる継続確認通信に基づいて、前記アプリケーションソフトウェアの実行継続を許可するか否かを管理する継続実行管理部とが設けられているソフトウェア実行制御システム。

３２．　コンピュータを、アプリケーションソフトウェアの実行を制御する実行制御部と、前記アプリケーションソフトウェア及び前記実行制御部の動作状態をそれぞれ監視する監視部として、機能させるためのコンピュータプログラムであって、

前記実行制御部は、

管理用コンピュータと通信することによりユーザ認証を要求する機能と、

前記管理用コンピュータから受信した第１の情報に基づいて、前記アプリケーションソフトウェアを起動させる機能と、

前記管理用コンピュータとの間で継続確認通信を行う機能と、

前記継続確認通信によって前記アプリケーションソフトウェアの実行継続が禁止された場合は、前記アプリケーションソフトウェアの動作を停止させる機能と、

を備え、

前記監視部は、

前記アプリケーションソフトウェア及び前記実行制御部の動作状態をそれぞれ監視する機能と、

前記アプリケーションソフトウェアまたは前記実行制御部のいずれか一方が動

作を停止した場合は、前記アプリケーションソフトウェア及び前記実行制御部をそれぞれ停止させ、自身も停止させる機能と、

を備えているコンピュータプログラム。

３３．　前記実行制御部は、さらに、

前記アプリケーションソフトウェア及び前記監視部の動作状態をそれぞれ監視する機能と、

前記アプリケーションソフトウェアまたは前記監視部のいずれか一方が動作を停止した場合は、前記アプリケーションソフトウェア及び前記監視部をそれぞれ停止させ、自身も停止させる機能を備えている請求項３２に記載のコンピュータプログラム。

３４．　前記実行制御部の前記継続確認通信を行う機能は、前記管理用コンピュータから予め設定された所定の時期に、前記管理用コンピュータから予め設定された第１の識別情報を前記管理用コンピュータに送信するものである請求項３２に記載のコンピュータプログラム。

３５．　前記継続確認通信を行う度に、前記管理用コンピュータから前記所定の時期が可変に設定される請求項３４に記載のコンピュータプログラム。

３６．　前記アプリケーションソフトウェアと、前記実行制御部と、前記監視部とは、同一の記録媒体に記録されて流通するものである請求項３２に記載のコンピュータプログラム。

FIG. 1

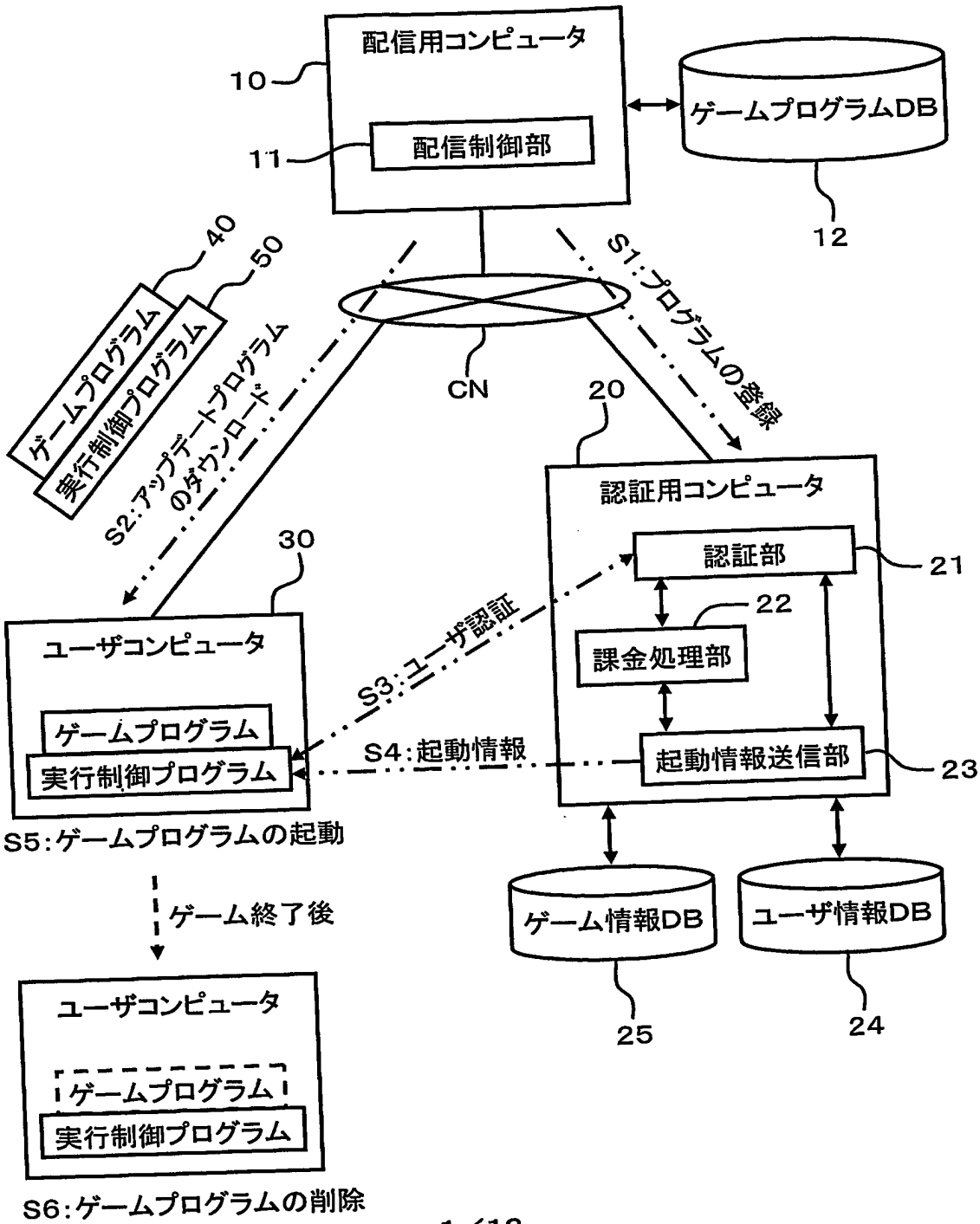

配信用コンピュータ
10
11
配信制御部
ゲームプログラムDB
12
40
50
ゲームプログラム
実行制御プログラム
S1:プログラムの登録
S2:アップデートプログラムのダウンロード
CN
20
認証用コンピュータ
認証部
21
22
課金処理部
30
ユーザコンピュータ
S3:ユーザ認証
ゲームプログラム
実行制御プログラム
S4:起動情報
起動情報送信部
23
S5:ゲームプログラムの起動
ゲーム終了後
ゲーム情報DB
ユーザ情報DB
25
24
ユーザコンピュータ
ゲームプログラム
実行制御プログラム
S6:ゲームプログラムの削除

FIG. 2

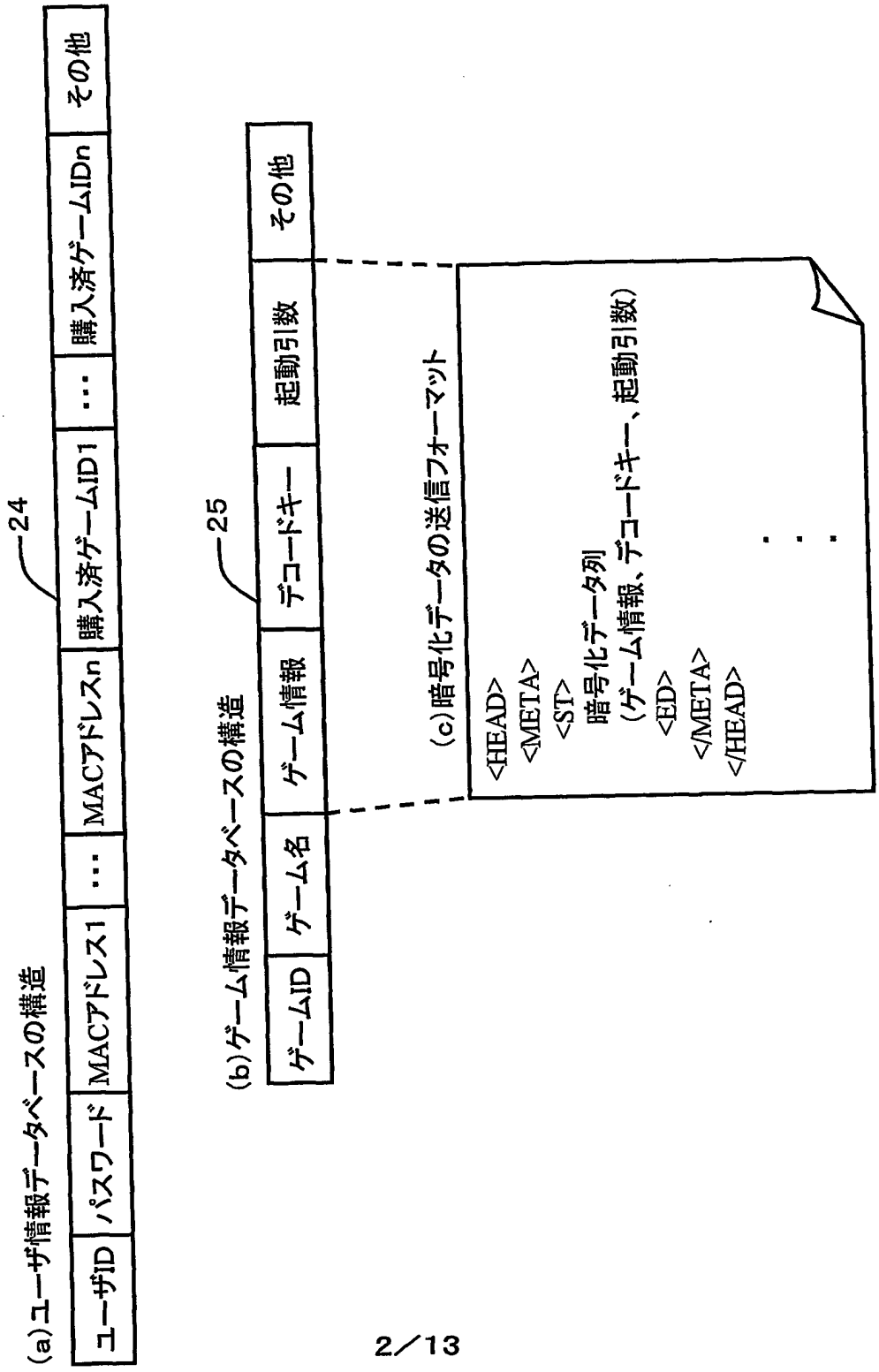
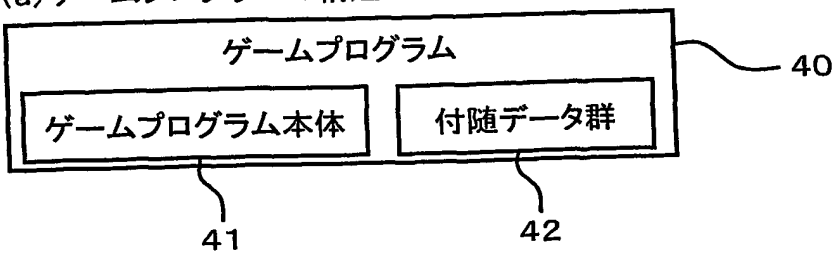

(a)ユーザ情報データベースの構造
24
ユーザID
パスワード
MACアドレス1
…
MACアドレスn
購入済ゲームID1
…
購入済ゲームIDn
その他
(b)ゲーム情報データベースの構造
25
ゲームID
ゲーム名
ゲーム情報
デコードキー
起動引数
その他
(c)暗号化データの送信フォーマット
<HEAD>
<META>
<ST>
暗号化データ列
(ゲーム情報、デコードキー、起動引数)
<ED>
</META>
</HEAD>
. . .

FIG. 3

(a)ゲームプログラムの構造



(b)実行制御プログラムの構造

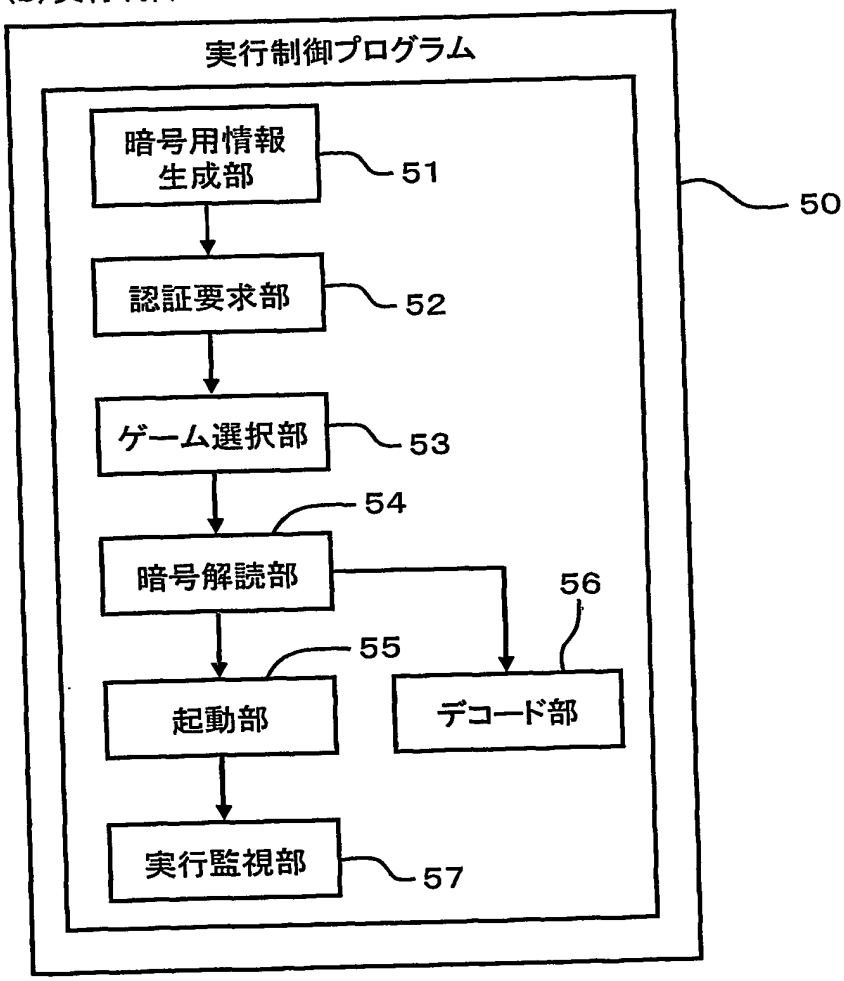


FIG. 4

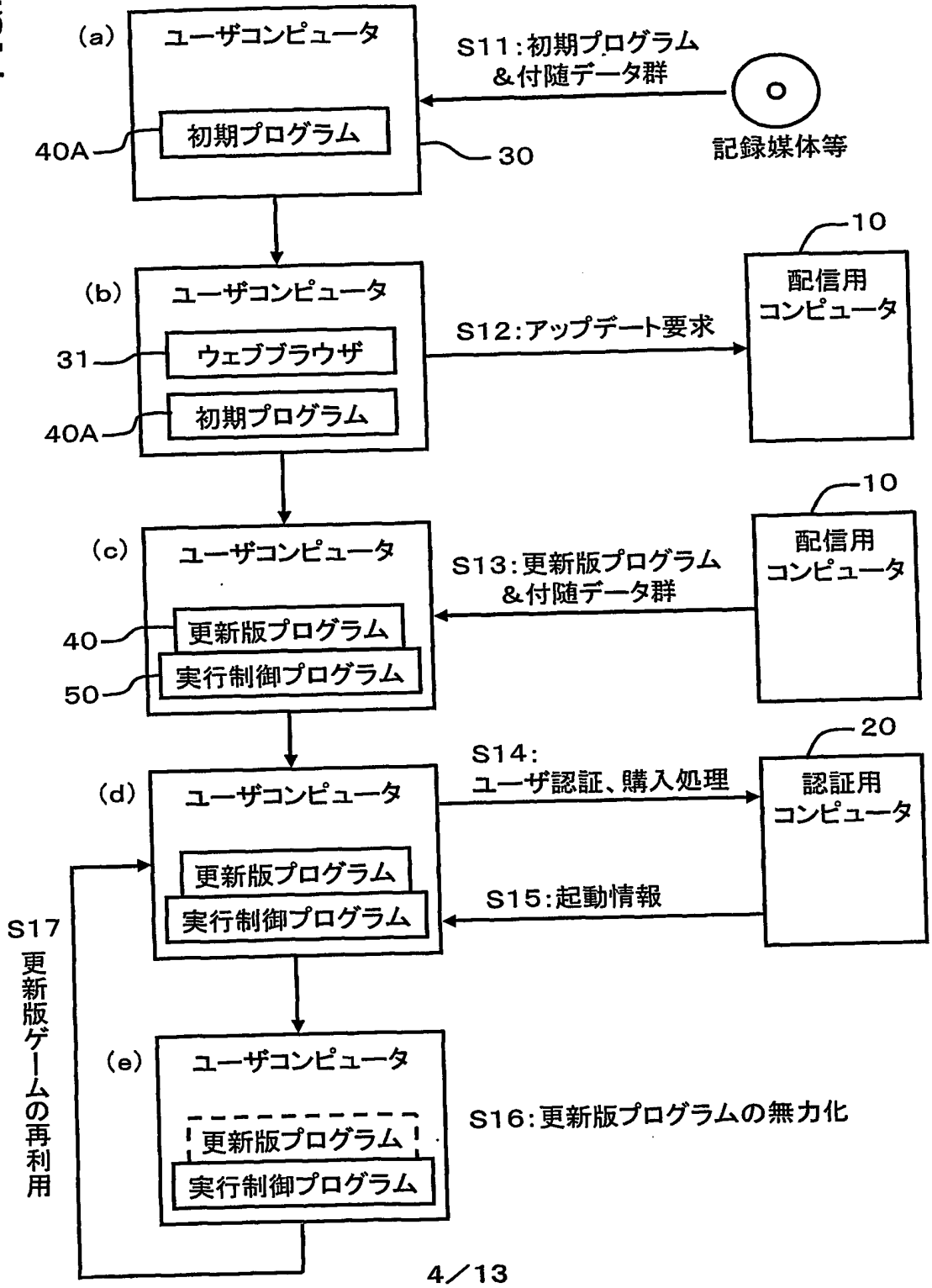

(a)
ユーザコンピュータ
初期プログラム
40A
30
S11:初期プログラム
&付随データ群
記録媒体等
(b)
ユーザコンピュータ
ウェブブラウザ
31
初期プログラム
40A
S12:アップデート要求
10
配信用
コンピュータ
(c)
ユーザコンピュータ
更新版プログラム
40
実行制御プログラム
50
S13:更新版プログラム
&付随データ群
10
配信用
コンピュータ
(d)
ユーザコンピュータ
更新版プログラム
実行制御プログラム
S14:
ユーザ認証、購入処理
S15:起動情報
20
認証用
コンピュータ
S17
更新版ゲームの再利用
(e)
ユーザコンピュータ
更新版プログラム
実行制御プログラム
S16:更新版プログラムの無力化

FIG. 5

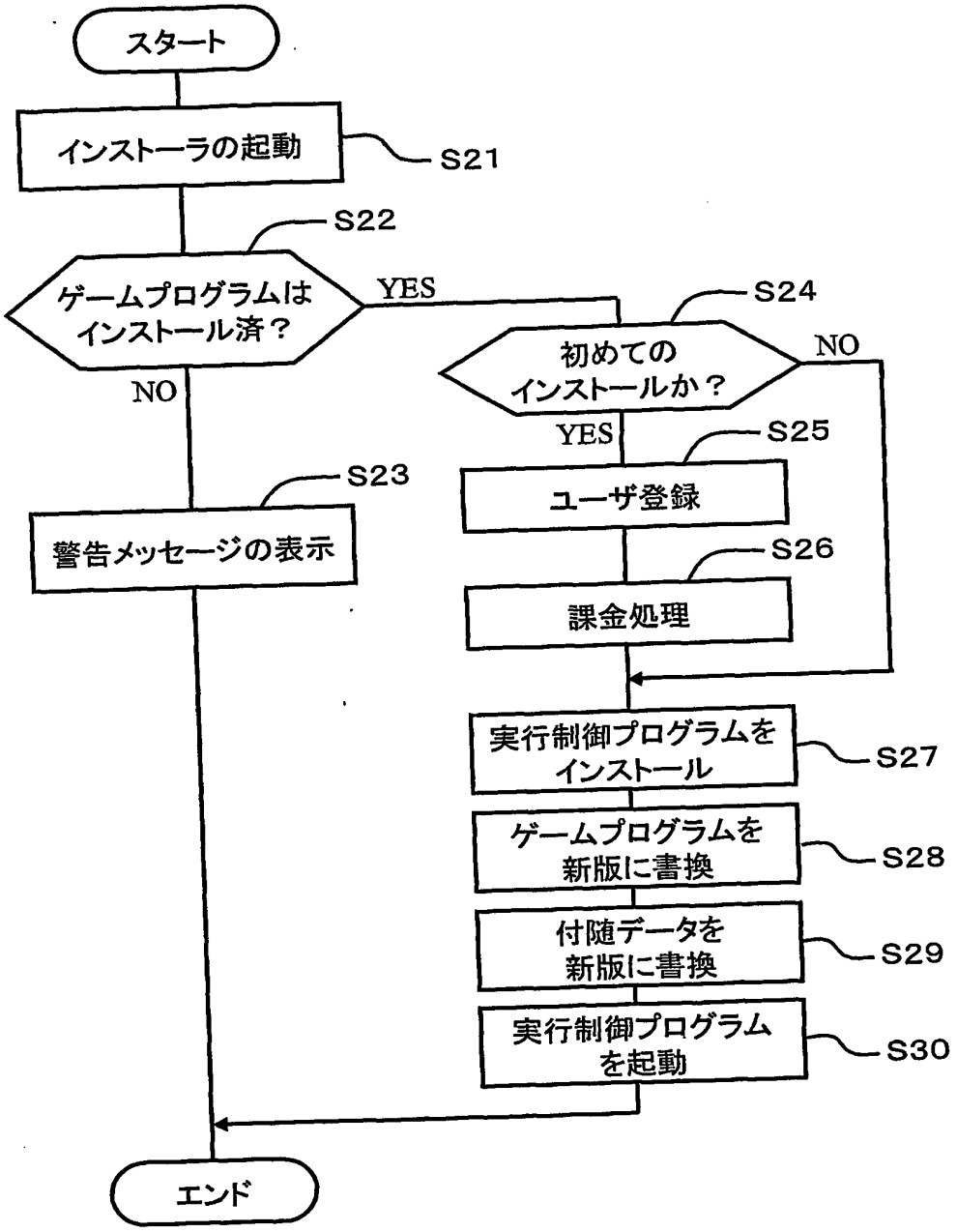

スタート
インストーラの起動
S21
S22
ゲームプログラムは
インストール済？
YES
NO
S24
初めての
インストールか？
NO
YES
S25
ユーザ登録
S26
課金処理
S23
警告メッセージの表示
実行制御プログラムを
インストール
S27
ゲームプログラムを
新版に書換
S28
付随データを
新版に書換
S29
実行制御プログラム
を起動
S30
エンド

FIG. 6

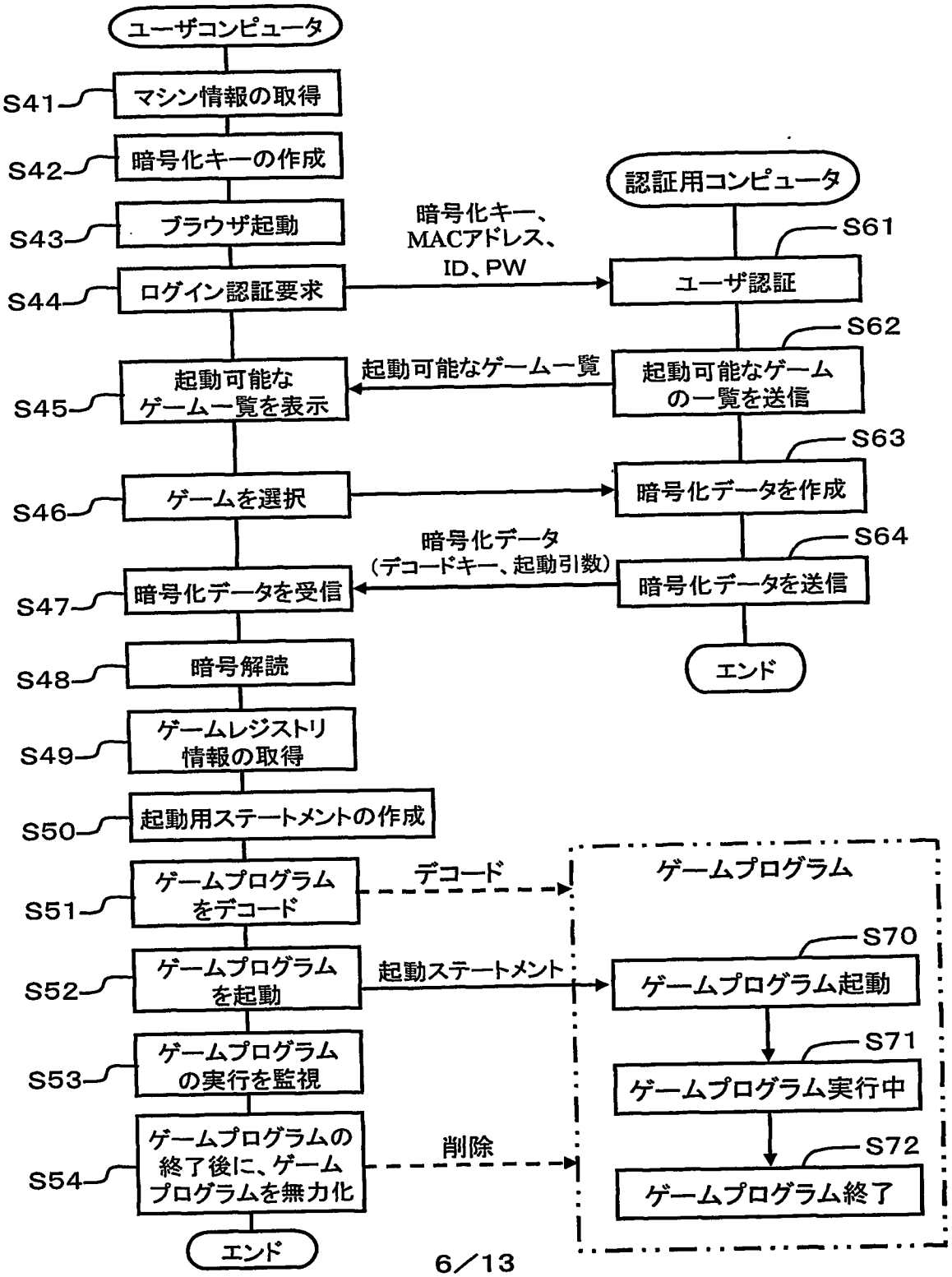

ユーザコンピュータ
S41
マシン情報の取得
S42
暗号化キーの作成
S43
ブラウザ起動
S44
ログイン認証要求
暗号化キー、
MACアドレス、
ID、PW
認証用コンピュータ
S61
ユーザ認証
S62
起動可能なゲーム
の一覧を送信
起動可能なゲーム一覧
S45
起動可能な
ゲーム一覧を表示
S63
暗号化データを作成
S46
ゲームを選択
暗号化データ
(デコードキー、起動引数)
S64
暗号化データを送信
S47
暗号化データを受信
エンド
S48
暗号解読
S49
ゲームレジストリ
情報の取得
S50
起動用ステートメントの作成
ゲームプログラム
S51
ゲームプログラム
をデコード
デコード
S52
ゲームプログラム
を起動
起動ステートメント
S70
ゲームプログラム起動
S53
ゲームプログラム
の実行を監視
S71
ゲームプログラム実行中
S54
ゲームプログラムの
終了後に、ゲーム
プログラムを無力化
削除
S72
ゲームプログラム終了
エンド

FIG. 7

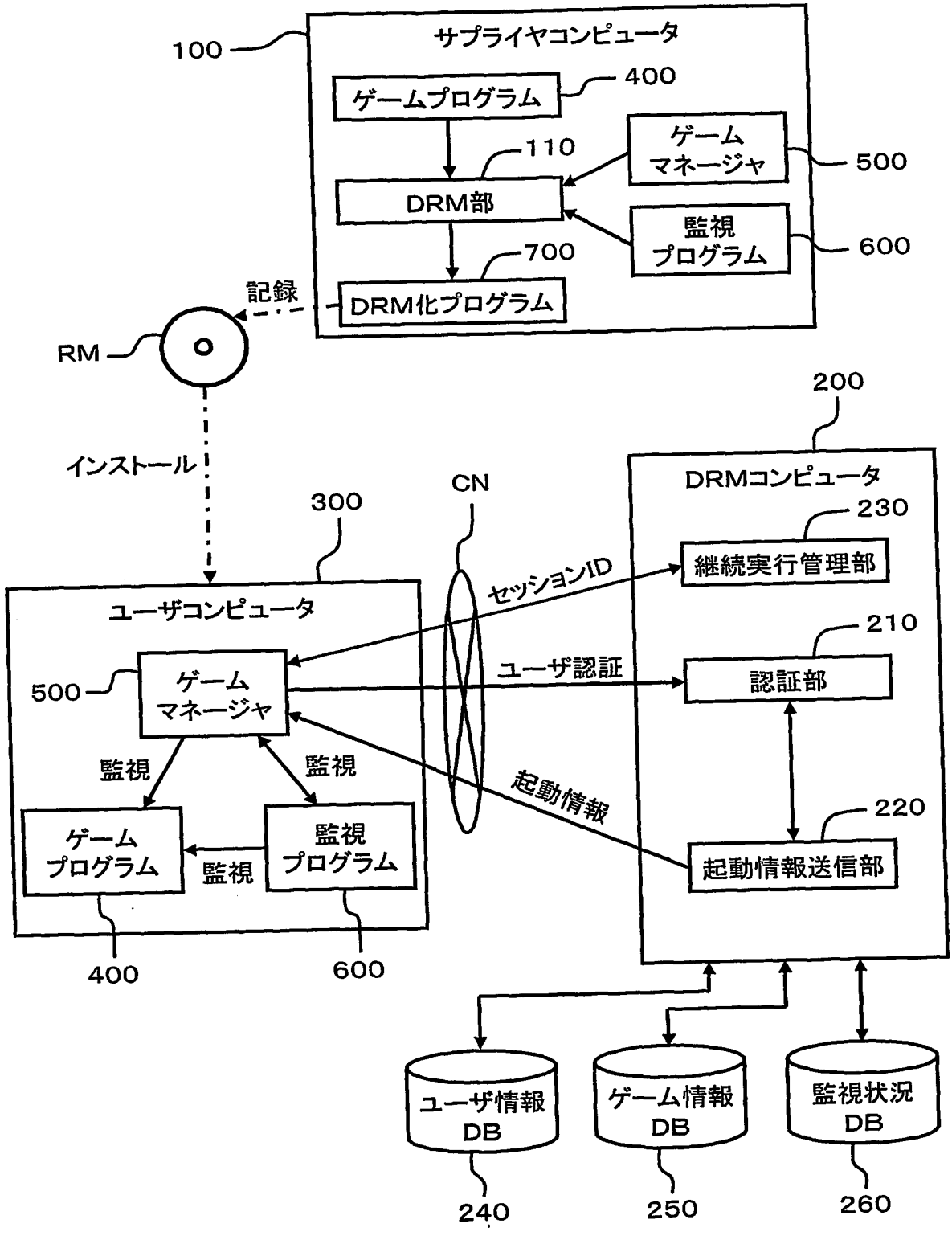

100
サプライヤコンピュータ
ゲームプログラム
400
ゲーム
マネージャ
500
110
DRM部
監視
プログラム
600
700
DRM化プログラム
記録
RM
インストール
200
DRMコンピュータ
CN
300
230
継続実行管理部
セッションID
ユーザコンピュータ
210
500
ゲーム
マネージャ
ユーザ認証
認証部
監視
監視
起動情報
220
ゲーム
プログラム
監視
監視
プログラム
起動情報送信部
400
600
ユーザ情報
DB
ゲーム情報
DB
監視状況
DB
240
250
260

FIG. 8

(a)

240

ユーザ情報データベース				
ユーザID	PW	MACアドレス	セッションID	その他
Interlex	Buddy	00-11-22-33-44-AA	Aaabbbcccddd...	

(b)

250

ゲーム情報データベース					
ゲームID	ゲーム名	ゲーム情報	デコードキー	起動引数	報告モード

報告モード
- 初回のみ
- 毎起動時
- 監視優先
- 負荷軽減

(c)

260

監視状況データベース					
ユーザID	報告周期	予定報告時期	ゲームID	ゲームスタート時刻	その他
ユーザ1	30分間隔	16:25	ゲーム1	13:01	
ユーザ2	40分間隔	16:00	ゲーム2	15:20	
ユーザ3	10分間隔	16:00	ゲーム3	15:30	

FIG. 9

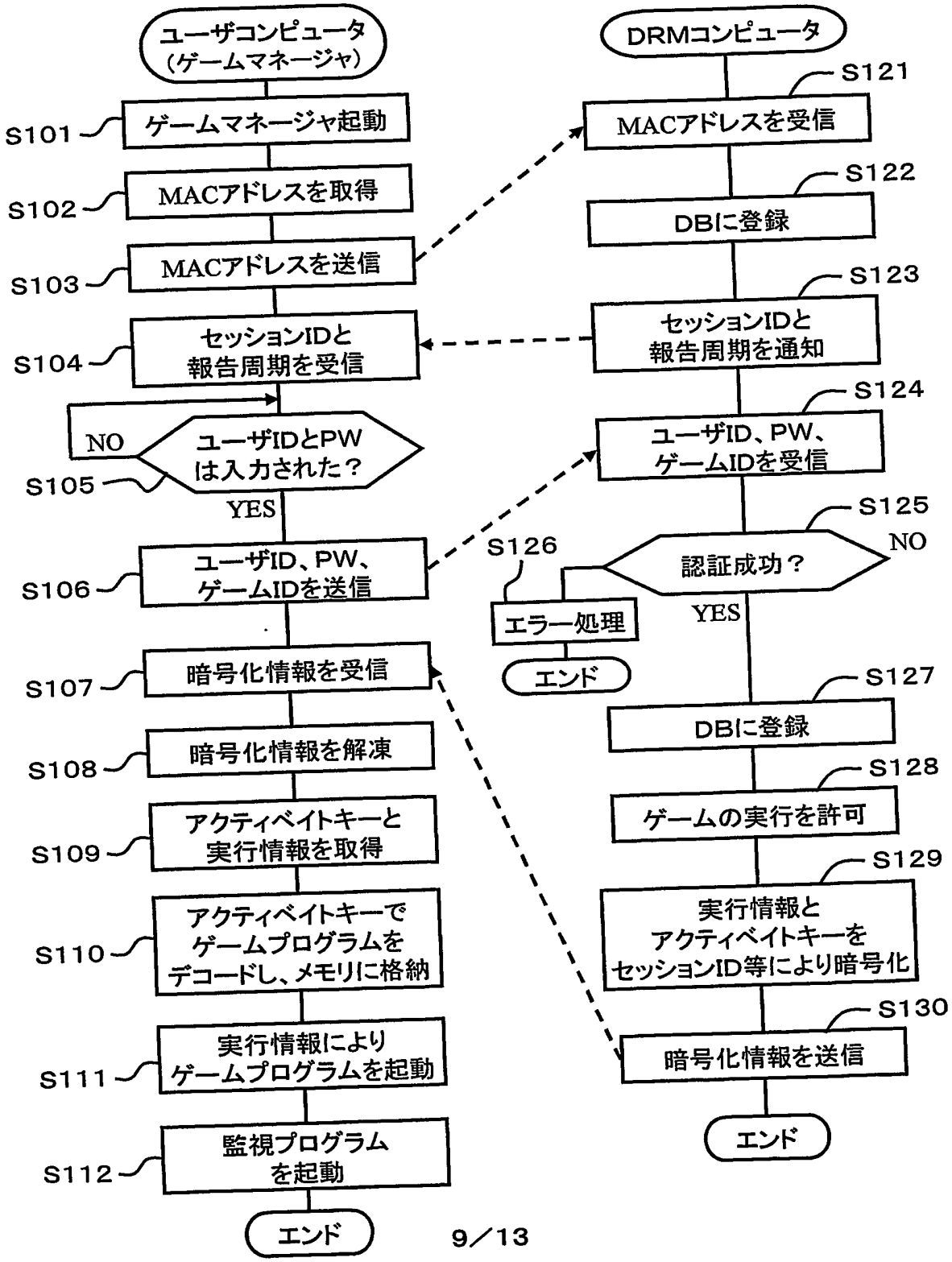

ユーザコンピュータ
(ゲームマネージャ)
S101
ゲームマネージャ起動
S102
MACアドレスを取得
S103
MACアドレスを送信
S104
セッションIDと
報告周期を受信
NO
ユーザIDとPW
は入力された？
S105
YES
S106
ユーザID、PW、
ゲームIDを送信
S107
暗号化情報を受信
S108
暗号化情報を解凍
S109
アクティベイトキーと
実行情報を取得
S110
アクティベイトキーで
ゲームプログラムを
デコードし、メモリに格納
S111
実行情報により
ゲームプログラムを起動
S112
監視プログラム
を起動
エンド
DRMコンピュータ
S121
MACアドレスを受信
S122
DBに登録
S123
セッションIDと
報告周期を通知
S124
ユーザID、PW、
ゲームIDを受信
S125
認証成功？
NO
S126
エラー処理
エンド
YES
S127
DBに登録
S128
ゲームの実行を許可
S129
実行情報と
アクティベイトキーを
セッションID等により暗号化
S130
暗号化情報を送信
エンド

FIG. 10

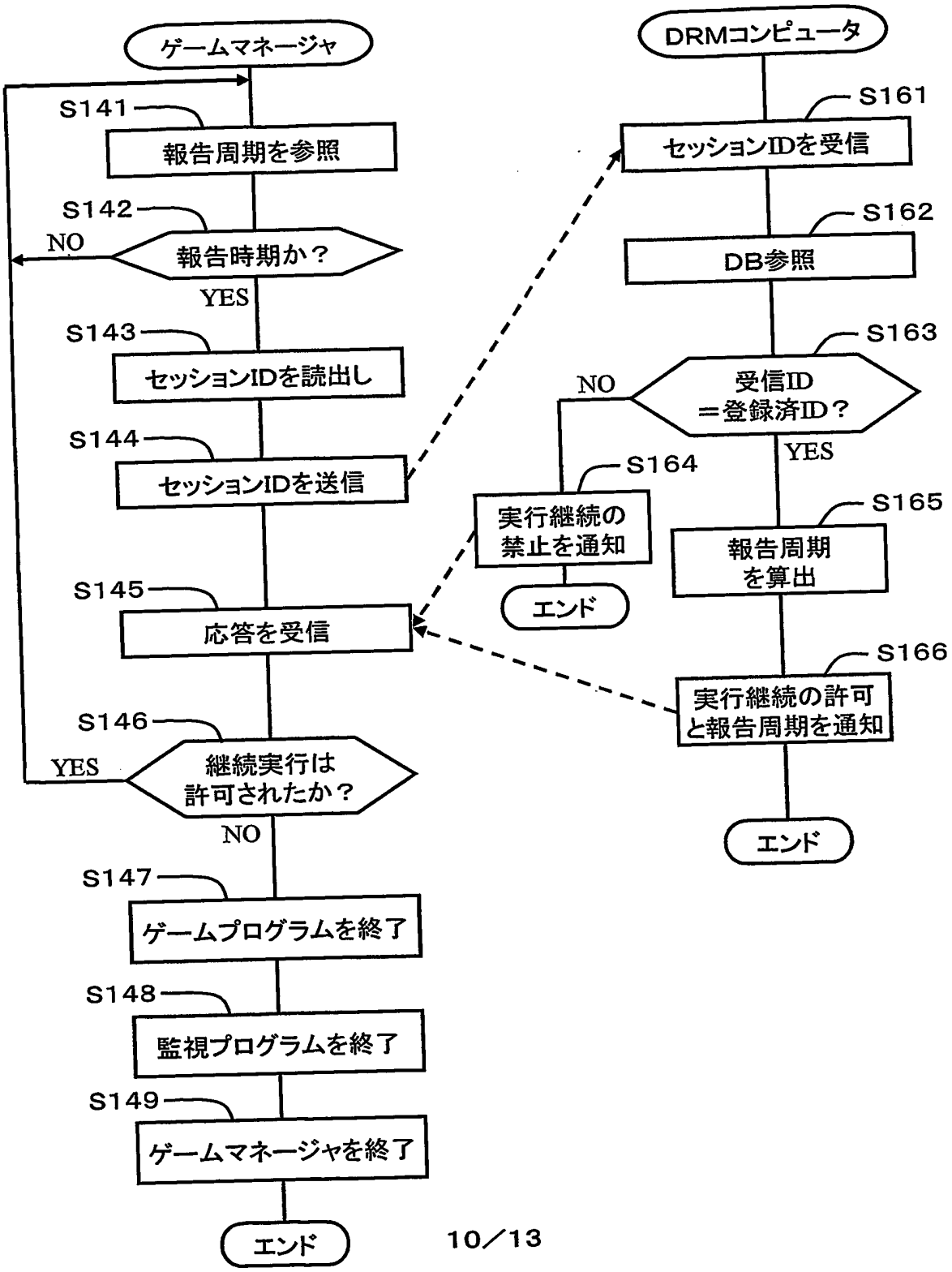

ゲームマネージャ
S141
報告周期を参照
S142
NO
報告時期か？
YES
S143
セッションIDを読出し
S144
セッションIDを送信
S145
応答を受信
S146
YES
継続実行は
許可されたか？
NO
S147
ゲームプログラムを終了
S148
監視プログラムを終了
S149
ゲームマネージャを終了
エンド
DRMコンピュータ
S161
セッションIDを受信
S162
DB参照
S163
NO
受信ID
＝登録済ID？
YES
S164
実行継続の
禁止を通知
エンド
S165
報告周期
を算出
S166
実行継続の許可
と報告周期を通知
エンド

FIG. 11

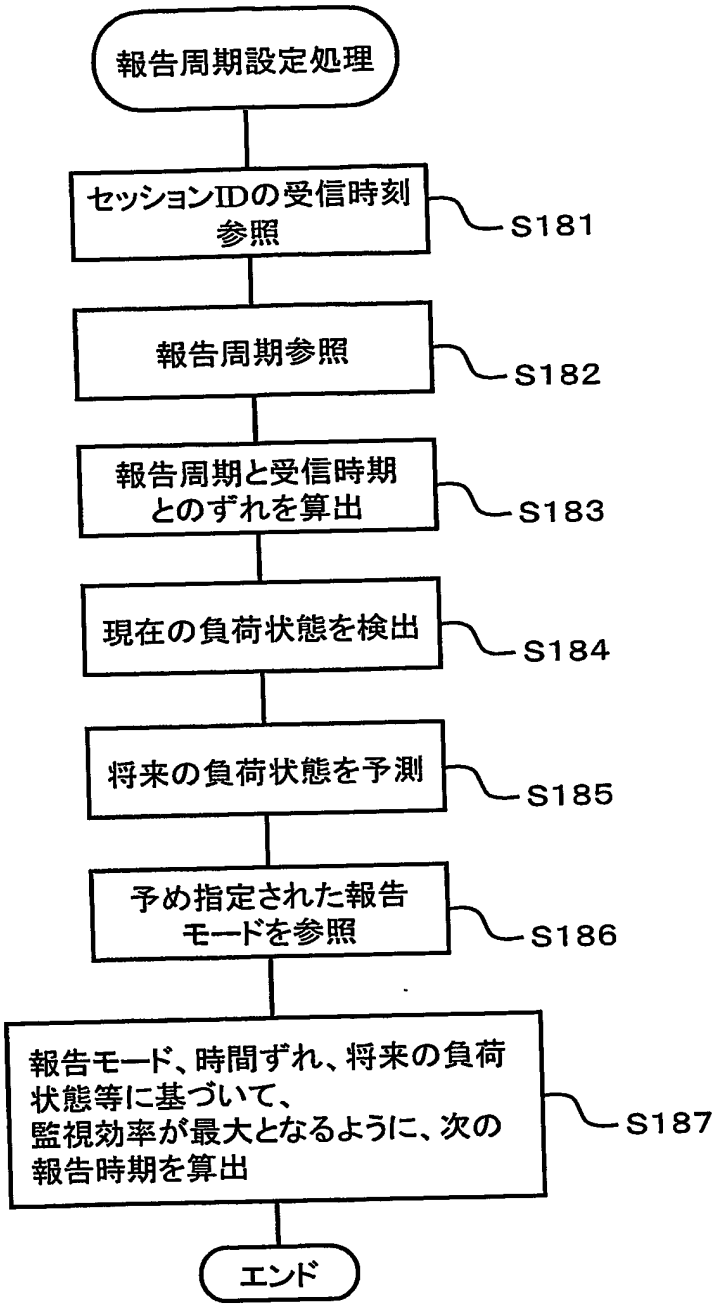

報告周期設定処理
セッションIDの受信時刻参照
S181
報告周期参照
S182
報告周期と受信時期とのずれを算出
S183
現在の負荷状態を検出
S184
将来の負荷状態を予測
S185
予め指定された報告モードを参照
S186
報告モード、時間ずれ、将来の負荷状態等に基づいて、監視効率が最大となるように、次の報告時期を算出
S187
エンド

FIG. 12

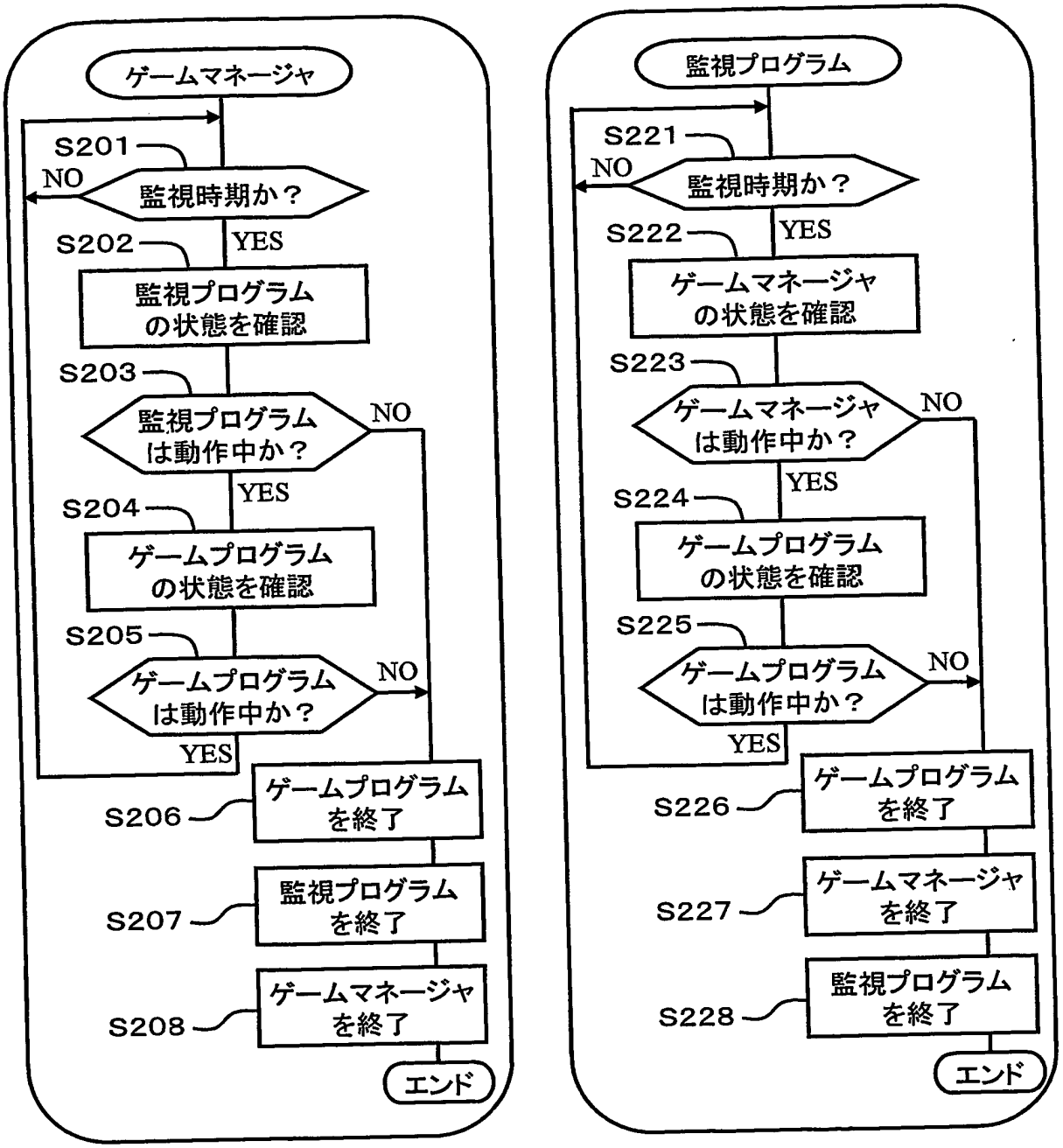
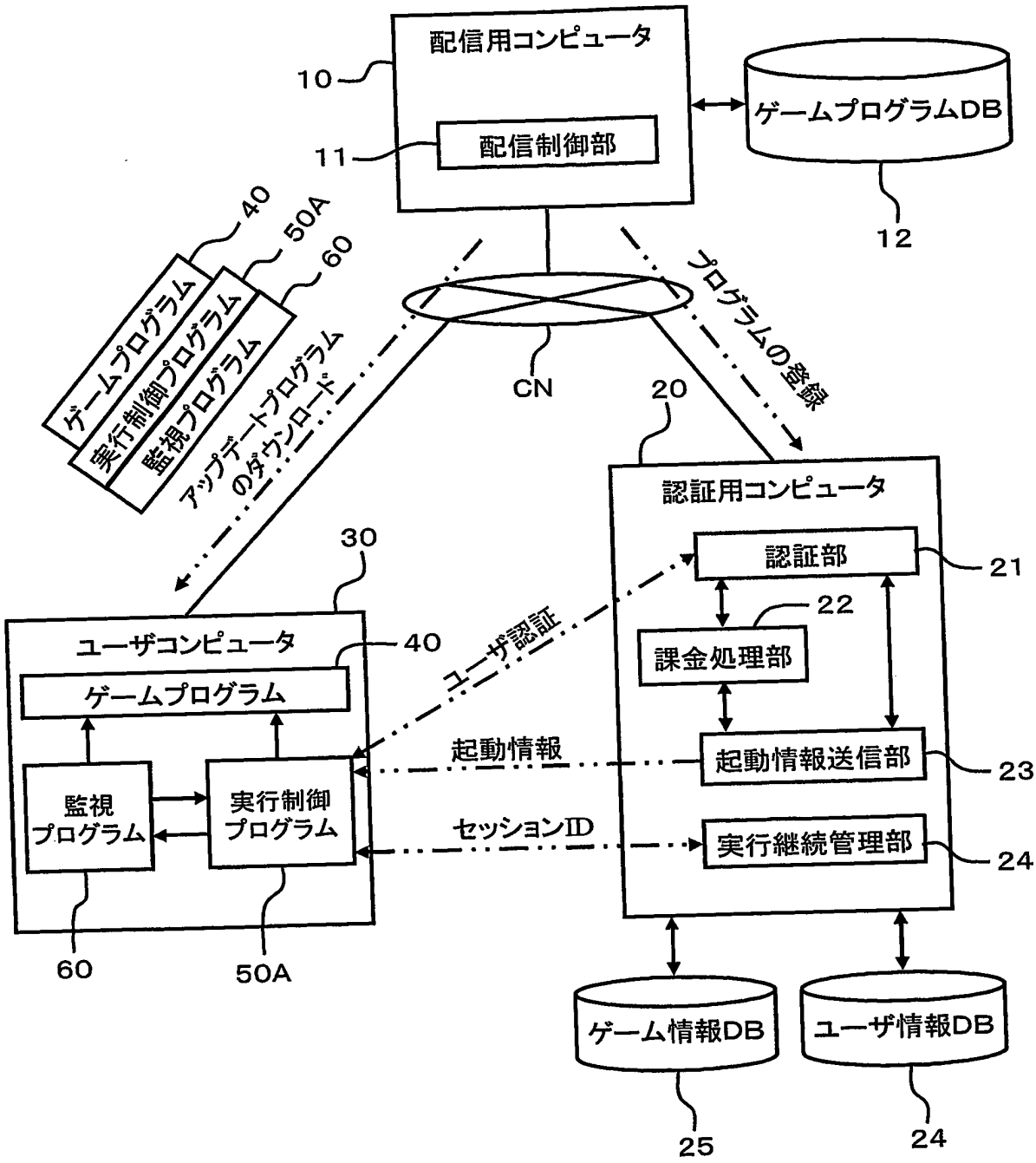

ゲームマネージャ
S201
NO
監視時期か？
YES
S202
監視プログラム
の状態を確認
S203
監視プログラム
は動作中か？
NO
YES
S204
ゲームプログラム
の状態を確認
S205
ゲームプログラム
は動作中か？
NO
YES
S206
ゲームプログラム
を終了
S207
監視プログラム
を終了
S208
ゲームマネージャ
を終了
エンド
監視プログラム
S221
NO
監視時期か？
YES
S222
ゲームマネージャ
の状態を確認
S223
ゲームマネージャ
は動作中か？
NO
YES
S224
ゲームプログラム
の状態を確認
S225
ゲームプログラム
は動作中か？
NO
YES
S226
ゲームプログラム
を終了
S227
ゲームマネージャ
を終了
S228
監視プログラム
を終了
エンド

FIG. 13


配信用コンピュータ
10
11
配信制御部
ゲームプログラムDB
12
40
50A
60
ゲームプログラム
実行制御プログラム
監視プログラム
アップデートプログラム
のダウンロード
CN
20
プログラムの登録
認証用コンピュータ
30
認証部
21
22
課金処理部
ユーザコンピュータ
40
ゲームプログラム
ユーザ認証
起動情報
起動情報送信部
23
監視
プログラム
実行制御
プログラム
セッションID
実行継続管理部
24
60
50A
ゲーム情報DB
ユーザ情報DB
25
24

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/15779

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F1/00, 12/14, 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-229660 A (Toshiba Corp.), 16 August, 2002 (16.08.02), Full text; Figs. 1 to 5 (Family: none)	1-23
Y	JP 10-133869 A (Shin'ichiro OGAWA), 22 May, 1998 (22.05.98), Full text; Figs. 1 to 2 (Family: none)	1-23
Y	JP 8-6784 A (Nippon Telegraph And Telephone Corp.), 12 January, 1996 (12.01.96), Full text; particularly, Par. No. [0053]; Figs. 1 to 3 (Family: none)	1-23

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 23 February, 2004 (23.02.04)	Date of mailing of the international search report 02 March, 2004 (02.03.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/15779

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 00/72119 A2 (Rabin, M.O. & Shasha, D.E.), 30 November, 2000 (30.11.00), Full text; Figs. 1 to 15 & CA 2368861 A & AU 4813700 A & EP 1180252 A2 & CN 1361882 T & JP 2003-500722 A	11-14,24-36
Y	JP 2001-84137 A (Matsushita Electric Industrial Co., Ltd.), 30 March, 2001 (30.03.01), Par. No. [0089]	7,17
Y	Par. Nos. [0053] to [0056] (Family: none)	13,28,29,35
A	JP 2002-163578 A (Kabushiki Kaisha Kuredisuto), 07 June, 2002 (07.06.02), Full text; Figs. 1 to 21 (Family: none)	1-36
A	JP 2002-351564 A (NTT Communications Kabushiki Kaisha), 06 December, 2002 (06.12.02), Full text; Figs. 1 to 11 (Family: none)	1-36

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/15779

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
The inventions of claims 1-23 are characterized in that second software and an execution control program are distributed to a user computer, the second software is decoded by using predetermined information and replace it with first software, start information is created according to predetermined information so as to start the second software, and when the execution of the second software is terminated, it is incapacitated.

(Continued to extra sheet)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/15779

Continuation of Box No. II of continuation of first sheet(1)

The inventions of claims 24-36 are characterized in that continuation of execution of application software is allowed or not allowed according to continuation confirmation communication performed with the execution control program at a predetermined timing. Between the group of inventions of claims 1-23 and the group of inventions of claims 24-36, there exists no other common feature which can be considered as a special technical feature within the meaning of PCT Rule 13.2, second sentence. Accordingly, no technical relationship within the meaning of PCT Rule 13 between the different inventions can be seen.

Consequently, claims 1-36 do not satisfy the requirement of unity of invention.

国際調査報告

国際出願番号　PCT／JP03／15779

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F 1／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F 1／00, 12／14, 15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国登録実用新案公報	1994－2004年
日本国実用新案登録公報	1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2002－229660 A（株式会社東芝） 2002.08.16、全文、第1－5図（ファミリーなし）	1－23
Y	JP 10－133869 A（小川伸一郎） 1998.05.22、全文、第1－2図（ファミリーなし）	1－23
Y	JP 8－6784 A（日本電信電話株式会社） 1996.01.12、全文（特に段落【0053】）、 第1－3図（ファミリーなし）	1－23

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　23.02.2004	国際調査報告の発送日　02.3.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5B　9193 林　毅 電話番号　03－3581－1101　内線　3546

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０３／１５７７９

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＷＯ　００／７２１１９　Ａ２ （Rabin, M. O. & Shasha, D. E.）、２０００．１１．３０、 全文、第１－１５図 & CA 2368861 A & AU 4813700 A & EP 1180252 A2 & CN 1361882 T & JP 2003-500722 A	11-14、24-36
Ｙ	ＪＰ　２００１－８４１３７　Ａ（松下電器産業株式会社） ２００１．０３．３０ 段落【００８９】	７、１７
Ｙ	段落【００５３】－【００５６】 （ファミリーなし）	13、28、29、35
Ａ	ＪＰ　２００２－１６３５７８　Ａ（株式会社クレディスト） ２００２．０６．０７、全文、第１－２１図（ファミリーなし）	１－３６
Ａ	ＪＰ　２００２－３５１５６４　Ａ （エヌ・ティ・ティ・コミュニケーションズ株式会社） ２００２．１２．０６、全文、第１－１１図（ファミリーなし）	１－３６

国際調査報告

国際出願番号ＰＣＴ／ＪＰ０３／１５７７９

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－２３に係る発明は、第２のソフトウエアと実行制御プログラムをユーザコンピュータに配信し、所定の情報を用いて第２のソフトウエアをデコードして第１のソフトウエアに置き換え、所定の情報に基づいて起動情報を生成して第２のソフトウエアを起動し、第２のソフトウエアの実行が終了するとこれを無効化することを特徴とし、請求の範囲２４－３６に係る発明は、所定の時期に実行制御プログラムとの間で行われる継続確認通信に基づいてアプリケーションソフトウェアの実行継続を許可するか否かを管理することを特徴とするから、請求の範囲１－２３に係る発明と、請求の範囲２４－３６に係る発明との間には、ＰＣＴ規則１３．２の第２文の意味において、特別な技術的特徴と考えられる他の共通事項は存在しないので、これらの発明の間にＰＣＴ規則１３の意味における技術的な関連を見いだすことはできない。

よって、請求の範囲１－３６は、発明の単一性の要件を満たしていない。

1．☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。